Barriers of trust in information sharing networks

Margrete Raaum

Masteroppgave
Master i Teknologi - Medieteknikk
30 ECTS
Avdeling for informatikk og medieteknikk
Høgskolen i Gjøvik, 2011

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Barriers of trust in information sharing networks

Margrete Raaum

2011/12/01

Abstract

The research area in question in this thesis is an analysis of success factors in information sharing trust networks that are designed to combat cyber crime. Information sharing is one of the key elements in successful security work, both in intrusion prevention as well as detection and incident handling.

Information sharing has been addressed by numerous national institutions, and also international bodies like the EU committees CEPS and ENISA. However, many of the research questions posed are of a technical nature, focusing on the technical side of creating an information sharing regime. Trust is just as important, and it partly replaces control. Based on interviews with key persons in security organizations, and on literature review, we look into elements of trust culture and the impact these have on a successful information network. We raise questions on the importance and facilitation of personal trust, and the impact of laws and regulations governing these areas, considering the lack of defined judiciary and of possible reprisals in trust communities. We look into the complex area of trust of intent, the constraints this puts on group size, and the complications of having participation by representation. We take into consideration relevant trust inhibitors and -enablers, both in terms of culture, communication mechanisms and trust network structure, and we consider whether political correctness can be an inhibitor of trust. We also provide some trust network recommendations based on our research.

Acknowledgements

I would like to thank Professor Dr. Bernhard M. Hämmerli for encouraging me to write this thesis, and for being a good sparring partner throughout the process. I would also like to thank all the interviewees, who not only took time to meet me and answer my questions and come with valuable input, but also for being patient and answering follow-up questions.

This thesis has been created using `gucmasterthesis` v0.8 as of 2011/12/01.

Margrete Raaum, 2011/12/01

Contents

List of Figures

1 Introduction

The thesis is organized in six chapters. In the first chapter we present the research area and our hypotheses. In Chapter 2 we do a review and comment some of the relevant literature on trust and trust networks and try to clarify the terms that will be used throughout the thesis. In Chapter 3 we review some of the work in the area of the research questions, and the results of the interviews are presented in Chapter 4. In Chapter 5 we discuss our findings, and we conclude in Chapter 6 with some recommendations, thoughts of future work and research evaluation. Acronyms and the original questionnaire are included as Appendix A and B. Throughout the thesis we have used the same personal pronoun, *she*, to neutralize or anonymize the statement or situation described.

1.1 Topics covered by thesis

Networked digital communication has become a necessity, and it is by many taken for granted and almost considered a basic human right. The complexity of networked communication increases as the critical systems in society increasingly become networked. These can be the systems normally labeled as Critical Infrastructure (CI), which comprises for instance power grids, oil rigs, railroads, air traffic systems or systems that carry personal sensitive information, like health care systems.

The amount of damage that can be inflicted on society by cyber attacks is proportional to the value of the system or the information carried by the system. The need to protect the networked assets becomes more and more acute. The motives for the perpetrators can be economical, like fraud, blackmail and theft, or it can be idealistic or political like espionage or sabotage. Whatever motives the attacker have, all strive to protect the systems, the network and the users from these criminals.

There are different approaches to defending oneself against these cyber crimes. Protecting the assets or hardening the systems to try to prevent the attackers from reaching their target is important. The second best thing to preventing attacks, is quickly detecting a breach of security or an attack to be able to take appropriate measures to counteract the effects.

In order to counteract attacks properly, one must be able to predict what kind of attacks could occur, and to do this one needs information about previous security incidents. Having sources of such information from outside your own network is a great advantage when assessing the threats. There are several initiatives to enable sharing of relevant information, like experiences from break-ins or logs of observed attacks, and there is a realization that many cyber criminals are well organized, and have an international network with effective information sharing.

The international collaboration for information sharing is difficult because knowing which data to share, as well as when and with whom to share becomes increasingly complicated. Useful information is often at a certain sensitivity level, and the exchanging parties are eager to keep the data within trusted perimeters. It is imperative to know who you can trust when working together

on incidents, or even just when preparing for future incidents. With the joint competence and efforts combating cyber crime, we should be able to share knowledge about trends and attacks, enabling us to harden the systems in time, or at least recognize an attack as soon as it starts.

1.2 Keywords

Information sharing, Trust, Relationship, Information hub, International joint ventures, Critical Infrastructure, Incidents, Culture, Network size, Network governance, Repairing trust

1.3 Problem description

Collaboration across borders can be challenging, due to cultural, political and economical differences, and some of these issues can seem hard to overcome in the process of building trust. At the same time: for the information shared between the parties to be truly useful, the information needs to be of a nature demanding a high level of trust between the exchanging parties.

There are sound frameworks and technical solutions for information sharing, like the framework developed by the Telecommunication Standardization Sector (ITU-T) [1] or the frameworks developed in the CERT communities. These do, however, not address the issues of personal trust and trust of intent. Technical trust, trust in the framework and in a person's or organization's identity is comparatively easy to obtain, it is mostly a technical challenge. Trust in intent is personal and based on experience, and from the first personal meeting, it takes time for trust to settle at a given level, depending on a number of factors. Even if the framework is place and the trust apparently has been established, lack of trust in one of the sharing parties will effectively block all information sharing.

An important factor in information sharing is personal trust, and this becomes increasingly harder to obtain as the group size increases, even if the network is built as a recommender system. There is a limit to the number of hops in transitive trust, as recorded in several articles by Jøsang et al.[3]. Trust network management or governance should be given more consideration than it is given today in many existing trust networks. Trust networks tend to grow big, and the network management is eager for the network to grow because it increases the organization's influence, politically and economically. If the network size is not planned for, this will probably lead to growing pains.

We see that groups that become too big for personal trust sometimes change, by for example splitting up into smaller groups. We also see examples of the trust network only being used as a contact network to enable the creation of smaller groups. One could impose a participation by representation only (a hierarchical model), but experience shows that this is difficult as not only does the trust of intent between representor and representee have to be absolute, but the representee needs both to trust the competence of the representor and to accept not having a personal voice in the trust network.

There is a desire with larger nations and corporations to create a cyber crisis network, so that in an emergency they can e.g. "call Europe". This coincides with the desire of large corporations to have fewer contacts to whom they have to report security issues. Being forced to communicate with every small player in the world might push larger corporations into being more exclusive on what and with whom to share, which in turn would lower the quality of information shared.

If, to answer these demands, a hierarchical organization is chosen, one should be aware of the complications.

Trust networks are formed in many compartments, for instance per sector, within large companies, in critical infrastructure protection or in education. To get a true picture of the threats, sharing networks should be public-private[1], since the infrastructure is largely privately owned, as discussed by Servida[4], and as many sectors as possible should be present.

Trust can not be forced, and trying to do so may actually diminish the trust level (see De Dreu et al.[5] on disruptive effects of punitive capability), so collaborating on best practices rather than rules and regulations with reprisals (see Hämmerli[6]), seems to be a more sensible way to support trust. A trust group always has implicit rules, and they change over time. The trust management in groups is an important process, as people join or leave the group. There must be an organized or at least an implicit way of handling these changes.

There are many barriers to trust and to be able to sustain a flow of useful information in a network the trust has to be at a certain level, and it should be constantly managed to avoid unnecessary drops in trust level.

1.4 Justification, motivation, benefits

Information sharing is vital in the battle against cyber criminals. No single organization or company sees enough data, or has by itself sufficient competence to understand the complete threat picture. If data is shared all involved can benefit from this. It will render them able to not only secure the information more soundly but also detect perpetrators before substantial damage is done. In critical infrastructure this can involve life threatening situations (powers sources, health care data etc).

Several organizations work to get the sharing of useful information flowing more actively than it is today. It all comes down to trust, whether the sharing party trusts the parties with whom they are about to share data, whether they trust the data shared with them and whether they trust others to make an effort as well. The latter element turns out to be a key factor; the activity in the networks are in general too low and this does not benefit the trust level.

As the networks grow more and more multi-cultural, this also turns out to be something to consider in evaluating trust network dynamics. This is potentially a touchy area, but we believe that political correctness can be a barrier for trust. An entirely different barrier that should not be underestimated is the lack of international legislation, and the complications of being law abiding in an international network.

As information sharing networks evolve, it is useful to examine the measures that have been deployed to enhance trust. We will evaluate which measures served their purpose, which did not, and to look for new suitable steps that might be taken.

[1] "Public-private" networks are networks consisting of both government and private sector companies.

1.5 Research questions

We will in this section go through our research questions, and the resulting hypotheses that were basis for the questionnaire used in the interviews. Through the initial research, these ares emerged: network size and type, trust network dynamics and governance, network activity and barriers to trust. These problem areas became the framework for the hypotheses.

1.5.1 Network size and network types

In normal social relations there is a limit to the amount of trusted peers one individual has. The private trust relations are not organized or governed as trust networks are, but we believe there are size limits to these networks as well. Our research question is:

How can one create a structure within the trust networks to decrease group size and hence enhance trust, and is a decrease the only option?

Hypothesis 1: Some of the trust networks of today are growing rapidly in size, and the trust level in the networks seem to decrease, and we hypothesize:

There is a size limit to trust and real trust is not possible in large groups.

Hypothesis 2: We do see the unique value in the existing multi-national networks, and see that the dynamic in the groups shifts to accommodate the size challenges, therefore:

A possible good solution to size issues is to restructure forming smaller units.

Hypothesis 3: Forming a hierarchical network, with participation by representation (delegate model) is often seen as a solution to restructuring to accommodate size issues, however in our experience this model has several complications, hence:

Creating and sustaining real trust in hierarchical networks is difficult and many times impossible.

1.5.2 Network dynamics and governance

The trust level in information sharing networks fluctuates, a phenomenon which is unfortunate for information sharing activities. The ideal situation would be a predictable trust level:

How can one manage trust dynamics in the event of (sudden) trust change in a trust community?

Hypothesis 4: We believe that it is difficult to repair trust in a network when it has been torn down, due to for example breaches of trust, switching of network members or introduction of new members:

An incident that breaches trust will naturally cause a downgrading of the trust level in the network.

Hypothesis 5: The governance of a network is important if it grows to more than a handful of members, but we believe that real trust networks are not controlled from the top. However we find the leader role to be important:

The leader role in a network needs to be strong and clearly defined.

1.5.3 Activity and network value

A network is all about the members and what they bring to the table, therefore we ask:

How does the network activity affect the trust network?

Hypothesis 6: Potential members need an incentive to become members in the network and to share, we postulate:

The main incentive for joining trust networks is to receive information and if this is true, then the network will die and trust disappears if there is no activity.

Corollary: *If information is not shared between members the network is obsolete*.

Hypothesis 7: There is never enough activity in a network to be able to test all scenarios, so in many cases exercises are organized to simulate incidents. However this is a situation where people pretend there is an incident, and believe this is not possible to do properly, hence:

Exercises is not a good tool to create network activity to build trust.

1.5.4 Barriers to trust

The networks in question are made for information sharing and there are clearly some barriers for trust and information sharing apart from network size. Cultural differences can also be relevant in this context as several networks are multi-national.

What are the major barriers of trust in a network and how does cultural factors affect trust and information sharing?

Hypothesis 8: Some of the information shared in a network may be legal in one country and illegal in another. This might become a conflict of interest for members, especially in law enforcement. The presence of law enforcement in trust networks may put a strain on members and prevent them for sharing information:

Law enforcement and regulatory authorities should not be members of regular information sharing networks.

Hypothesis 9: In large multi-national networks, members from vastly different cultures are supposed to work together. If they do not understand each other, either because of language issues or differences in values or behavior, this may not be easy. If these difficulties are not addressed because there is a wish to be polite and not talk about this, there will be no solution. We believe that:

Misunderstood political correctness in cultural diverse networks can destroy trust.

1.6 Choice of methods

In this chapter we describe the research method, as well as the ethical considertations and the confidentiality issues that were taken into account.

The goal was to choose the appropriate method to enlighten the problem at hand. There is a substantial amount of literature within the disciplines of psychology and sociology on different aspects of trust. On digital information sharing, there is a fair amount on the technical side of information sharing frameworks and trust management, but there is not much written on the sociological sides of digital information sharing, and as we regard real trust mainly as a psychological or sociological phenomenon, we wanted to base the thesis on input from experienced professionals.

The method chosen was semi structured interviews. Several iterative follow up rounds were performed as the questions turned out to be slightly inadequate to enlighten the subject properly, and also because new angles and questions arose during the interviews. The interviewees were security professionals of different backgrounds, all experienced in trust network building and the enabling of information sharing. Both empirical and theoretical outcome was expected.

Interviews were chosen as method as they are much more personal than online surveys, whether done by email or via a web page. In addition to ensuring that the interviewee actually answers the questions, it gives the researcher the possibility to pose follow-up questions, or even follow the interviewees' train of thought, especially since the facial expressions and body language are available.

1.6.1 The semi structured interview

We did not intend to try out an existing, well known hypothesis, in which case a quantitative approach would have been chosen. Instead we chose a qualitative approach as the inductive methodology, where the hypothesis are made from "educated guesses", which in turn are tested. We chose semi structured interviews as the interviewees are trained and creative professionals and information was expected to appear that would lead to new angles or new sets of questions, and a structured interview would hence lock down the creative process. On the other hand, a non structured interview would make it more difficult to create verifiability and repeatability, as the interviewees would not necessarily be answering all the same questions.

An interview guide was prepared, with a set of approximately 30 questions categorized in the main topics; group size, trust level dynamics, network activity and barriers to trust, see Appendix B. The guide was tested on a reference group, to check for inconsistencies and to identify follow-up questions that would arise during the interviews. The reference group was not composed of security specialists.

Doing the interviews over the telephone was a possibility, especially as the interviewer and interviewees for the most part already were acquainted. This obviously has its advantages in speed and availability, however we found the drawbacks to be substantial:

- Many people do not like to talk on the telephone
- Most of the interviewees and the interviewer were not speaking their native tongue, so this and even poor transmission could lead to misunderstandings

- Most people are more comfortable confiding in someone they can see, it creates trust, hence receiving open answers is easier

The choice of personal interview as form eliminate many of the potential challenges of ambiguous questions as clarifications can be made on the spot, and also the effect of social inhibitors and language problems decrease (Askheim and Grennes[7]).

Each interview was therefore carried out face to face, they lasted between 20 and 50 minutes, they were all conducted in surroundings were the interview could not be heard by interested bystanders and most of the interviews were taped, in case of need for clarification later, in the transcription process. All seven interviews were conducted and transcribed within six weeks to ensure continuity, and that nothing would be misinterpreted. The interviewees were sent the transcripts to enable feedback where corrections or clarifications were needed. The transcripts were sent encrypted where possible, and the corresponding files on the digital voice recorder used during the interviews were deleted in a secure manner.

1.6.2 The selection of the interviewees/sampling

All interviewees chosen fulfilled the following criteria:

- They were highly trained security professionals.
- They had many years of experience in the security community.
- They were members of different trust networks, and there was great diversity in the nature of the trust networks.
- They were highly trusted and respected internationally.
- They were chosen to cover educational networks, as well as business oriented, public and private, inside and outside the EU.
- Two separate cultures were represented. The interviewees were either European or Asian.
- They were asked to answer the questions as individuals and not as an employee, or as a trust network representative.
- Both sexes were represented.

1.6.3 The interview process

The interviewees were asked to participate, some by email and some in person while attending fellow trust network meetings.

To ensure sufficient trust in the interview process, the interviews were done in person. In the cases where the interviewer and the interviewee was not acquainted the interview was initiated by some information sharing by the interviewer as an ice breaker to increase the trust. As predicted, already the first interview revealed new and interesting directions and questions that we wanted to incorporate, hence the set of questions changed during the entire course of the interviews. The iterative process of the interview guide change enabled a creative and relaxed process, however creating a need for follow-up communication with the interviewees. Several interviewees were contacted multiple times with follow up questions.

1.6.4 Bias

The influence of the interviewers background was carefully considered, but was seen as an asset, and not a liability. The interviewer is a security professional, member of several trust networks, and professional acquaintance of most of the interviewees. This presumably enables a better understanding of the problem, and makes it easier to predict findings. We feel that the benefits of the existing trust outweighs the possible personal bias created by the existing relations.

We feel the choice of interviewees was well founded, as did the reference test group who was presented with the choice of interviewees.

We evaluated the individual interviewees foundation for answering each question. The interviewees were openly given an opportunity to not answer questions, if they felt their background was not well founded in that area, or if they did not have an opinion on the matter at hand. This was to avoid answers that would inhibit analytical generalization (Kvale[8]).

1.6.5 Ethics and confidentiality

Some of the potential challenges in fully informing the interviewees in qualitative research is discussed by Eisner[9], and we considered whether full access to the questionnaire could be given in advance (full consent), or whether this could slant the results. The resulting informed consent included a brief overview of the main three areas, because we did not wish for the interviewees to prepare for the individual questions.

In the interview process, statements were omitted if the wish for this was expressed by the interviewee. As mentioned: after the transcription the interviews were thoroughly erased from the recorder, notes taken were shredded and the transcriptions were sent encrypted to the interviewees for approval, comments and corrections. The transcripts will be kept electronically for the future, but encrypted.

The interviewees were promised full confidentiality, hence the transcripts are not included in the appendices, and the citations are anonymized, both regarding name, gender and workplace.

1.7 Some existing trust networks

In the next chapter we take a closer look at trust and trust network theory. Here, we briefly present some basic facts about a few of the existing official trust networks today. These networks were all included at some point as background studies in the thesis.

FIRST: Forum of Incident Response and Security Teams

Mission statement: *FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.*

Homepage: http://www.first.org/

Scope: Global

Number of members: 248 members

Potential members: Commercial, governmental or educational security teams, or individuals as special liaisons.

Membership requirements: A set of requirements, and all need two sponsors[2] among the existing full members.

Procedure for acceptance: Steering group votes to accept new members.

TI: Trusted Introducer

Mission statement: *The Trusted Introducer is the trusted backbone of the Security and Incident Response Team community in Europe. The TI lists, accredits and certifies teams, and provides them with a well-balanced set of trusted security services.*

Homepage: http://www.trusted-introducer.org/

Scope: Global, European-centric

Number of members: 85 accredited (3 certified), 67 listed

Potential members: Security teams, or individuals as special liaisons.

Membership requirements: A set of requirements, and all need two sponsors among the existing full members. The team has to be just “listed” for a period while the “accredited membership” criteria are met.

Procedure for acceptance: New members are accepted if they fulfill the requirements and no member protests.

[2] “Sponsor” in this context means some team or person who are willing to vouch for the applicants intentions, "vetting" mentioned earlier.

MELANI: Melde- und Analysestelle Informationssicherung

Mission statement: *Within MELANI, the Reporting and Analysis Centre for Information Assurance, partners work together who are active in the area of security of computer systems and the Internet and protection of critical national infrastructures.*

Homepage: http://www.melani.admin.ch/

Scope: Switzerland

Number of members: 100 companies, 2 specific people from each company.

Potential members: Security representatives from organizations in Swiss Critical Infrastructure

Membership requirements: MELANI assesses applications of companies and decides, whether a company qualifies as critical. Furthermore, MELANI usually asks standing members in a sector beforehand about possible new entries. The members remain hidden to others outside the network.

Procedure for acceptance: Melani central organization accepts and vets new members.

All information shared goes through the Melani central hub, where it is sufficiently anonymized and desensitized to be shared with other member. Sharing happens either on a one to one, one to sector or one to all members basis.

APCERT: Asia Pacific Computer Emergency Response Team

Mission statement: *APCERT cooperates with CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) to ensure Internet security in the Asia Pacific region based around genuine information sharing, trust and cooperation.*

Homepage: http://www.apcert.org/

Scope: Asia-Pacific region

Number of members: 27 members, membership is team based with a team representative that attends meetings.

Potential members: Security teams in the Asia Pacific region.

Membership requirements: All need at least one sponsor among the existing full members. The team has to be “general member” for some time before the team is accepted as “full member”.

Procedure for acceptance: Steering group votes to accept new members.

OIC-CERT: The Organisation of the Islamic Cooperation – Computer Emergency Response Team

Mission statement: *OIC-CERT provides a platform for member countries to explore and to develop collaborative initiatives and possible partnerships in matters pertaining to cyber security that shall strengthen their self reliant in the cyberspace.*

Homepage: http://www.oic-cert.net/

Scope: Organization of Islamic Cooperation

Number of members: 24 members (22 team representatives and 2 professionals, totally representing 18 countries)

Potential members:

- Full members: Any teams from the OIC countries that have the mandate to act on behalf of their government.
- General members: Security teams from the OIC countries
- Professional member: Security experts
- Affiliate members: Security teams from non OIC countries
- Commercial members: Cyber security industry

Membership requirements: Most need one sponsor among the full members, "affiliate" and "commercial" need two sponsors.

Procedure for acceptance: Steering committee votes to accept new members.

EGC: European Government CERTs

Mission statement: *The EGC group is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe.*

Homepage: http://www.egc-group.org/

Scope: Europe (not only EU)

Number of members: 13

Potential members: Incident Response Teams working for the government of European countries.

Membership requirements: That the team is a "governmental" CERT (ambiguous)

Procedure for acceptance: Mutual consent in the team

OPSEC-Trust

Mission statement: *OPSEC-Trust (or "ops-trust") forum is a highly vetted community of security professionals focused on the operational robustness, integrity, and security of the Internet. The community promotes responsible action against malicious behavior beyond just observation, analysis and research.*

Homepage: https://ops-trust.net/

Scope: Global

Number of members: Unknown

Potential members: Individuals “in a position to directly affect Internet security operations in some meaningful way”

Membership requirements: New candidates are nominated by their peers who must have worked with them.

Procedure for acceptance: Sufficiently vetted (number of recommendations and strength of links)

2 Trust characteristics research

According to Shaw[10], "Interpersonal relationships begin with the perception of others". From there, trust is built one step at a time. In this chapter we briefly explore some important research in the vast field of trust to pinpoint the most relevant aspects of trust for our problem and the impact this has on information sharing. We also look closer at the concept of trust networks, review important work in this area, and try to conclude on important aspects of these for further use in the work on the research questions.

2.1 Trust

Trust is a group phenomenon, but the desicion to trust is individual, and the factors that influence these processes are complex, and not even always conscious.

Zucker[11] postulates that trust is based on the process of exchange, characteristics of the exchange partners and societal institutions, and Doney et al.[12] conclude that trust is a set of beliefs or expectations, and a willingness to act on those beliefs judged from the individual's subjective evaluation of the probability of success. The trust decision itself is binary, to trust or not to trust, but there are several levels of trust, Ruohomaa and Kutvonen[13]. We do not consider authentication as trust in this context, it is merely a tool to manage authorization (Abdul-Rahman and Hailes[14]), and part of a framework of collaboration.

In a trust liaison we define the trust actors as the trustor (the one trusting) and the trustee (the one being trusted), and as (re)formulated by Msanjila and Afsarmanesh[15]:

- Trust is the willingness of a trustor to be vulnerable to the actions of another party based on the expectations that the trustee will perform a particular action important to the trustor irrespective of the ability to monitor or control the trustee (Mayer et al.[16]).
- Trust is the belief in the competency of an entity to act dependably, securely and reliably within a specified context (Grandison et al.[17]).
- Trust is a psychological condition comprising the trustor's intention to accept vulnerability based on positive expectation of trustee's intentions and behavior (Rousseau et al.[18]).

An individual can be perceived as trustworthy in different contexts, like economical (you would lend her money), socially (you would let her have an extra house key), managerial (experience, stability), technological (competence) and structural (internal structure) (Msanjila and Afsarmanesh[19]). Of these, the economical is probably the least relevant in this thesis.

In trust, three dimensions of the trustee's characteristics are considered: the trustee's ability, integrity and benevolence (Cosimano[20]). The first being not only a technical ability, but for instance the possibility of a third party forcing the trustee to act in a certain manner. The second

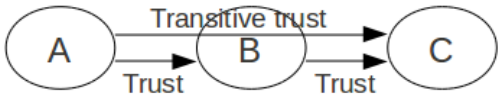

Figure 1: Trust has boundaries. In trust transitivity, trust propagates through trust actors, “by proxy”.

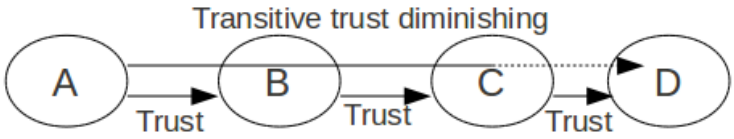

Figure 2: There are limits to how long transitive trust links can be, as the trust bandwidth will gradually approach zero.

being a transit that often becomes proven or disproved, and the third being difficult to prove, hence has to be “blindly” trusted.

We mentioned that trust is transitive, and that there is a limit to transitivity, see Figure 1 and Figure 2. If the trust chain becomes too long, the trust diminishes to unacceptable levels, Jøsang et al.[21], which is also intuitively so. You would not trust someone if the degree away from the recommended person was high (probably a problem if it is more than three).

The trust scope also depends on the context, Jøsang et al.[3], as mentioned above, for example whether it is sharing incident data or fetching the children from school.

Msanjila discusses rational vs. subjective trust. Rational is built on facts only, hence is not transitive. In subjective trust, as Massa & Avesani[22] point out: trustors can have different opinions about a trustee. Subjective trust is often based on recommendations, and is the relevant form of trust in this thesis. This corresponds to the “relational trust” treated by Rousseau et al.[18]. We do not look further at calculus-based trust, however the deterrence-based trust Rousseau et al. are discussing is interesting. This is not necessarily what we consider “real trust”, it depends of the punitive capabilities of the trustor, and is more relevant in non-trusted cooperation situations.

“Trust and risk are negatively related. When there is a high chance that certain risks can arise in an environment it is very hard for an organization to trust others in the environment” (Msanjila and Afsarmanesh[19]). However, paradoxically, an important conclusion is that a “fundamental condition of trust is that it must be possible for the partner to abuse the trust”, Dasgupta[23], and that “if one were omniscient, actions could be undertaken with complete certainty, leaving no need, or even possibility for trust to develop”, Deutsch[24]. This coincides with Rousseau et al.[18] who state that there can not be any trust without real risk. Uncertainty whether the other intends to and will act appropriately is the source of the risk. It creates the opportunity for trust which leads to risk taking. They also identify another necessary condition; interdependence. Rousseau et al. discuss that there must be reciprocity for trust to be built, and also conversely that risk taking “buttresses a sense of trust when the expected behavior materializes”.

There are cultural variations as to how much deviance from expectations, or amount of risk individuals tolerate. Some cultures demand more structure, rules and regulations than others (Doney et al.[12]).

A trustor's "propensity to trust" gives a level of how trusting the trustor is, and is influenced by cultural, social, developmental experiences as well as personality type, Jarvenpaa et al.[25]. Bachmann[26] backs this up and discusses not only cultural variations in personal trust but also trust in "the system" and "the law". Some of this is discussed by Kramer[27] as "rule-based trust".

Jarvenpaa et al.[25] stress that building trust takes time, labeled by Kramer[27] as "history-based trust" and this coincides with what we described earlier as experience-based trust. This is further explored by Msanjila et al.[19] as stages in trust development. Bachmann[26] sees personal trust as a starting point and if achieved, "system based" trust as advanced form of trust production, we discuss this briefly at the end of the chapter. Yuki et al.[28] discuss the effect of meeting face-to-face to form personal links contra the effect of just being in the same network in two different cultures, however we want to stress that face-to-face meetings are beneficial regardless of culture, as supported by Loss et al.[29]

As a curiosity, we observe that if a trustor is being too trusting, it reduces the trustworthiness of this individual. This is supported by Jarvenpaa et al. This would probably amount to the trustor appearing either of ill judgment or incompetent, discouraging the observers to trust the trustor with their valuable information.

Another factor of trust is an individual's skewed view of his or her own perceived and actual trustworthiness, most individuals consider themselves to be, and to be perceived as, more trustworthy than their peers. Both Jianghe Niu[30] and Elahee et al.[31] suggest it to be due to human nature, thinking we are better than others. We will not pursue this as the group- and cultural diversity in this area seems relatively small, Jianghe Niu[30], but it is something to keep in mind while analyzing trust behavior.

There is of course an individual personality side to a trustor, whether a person is particularly trusting or not, but this is beyond the scope of this paper.

2.2 Trust and information sharing

In this thesis, the objective of the trust is to enable the exchange of security related information to improve cyber security. This information not only include elements like incident detection and monitoring data, but also policy-related information. We view data as divided into "operational data", which is data pulled out from online systems, anonymized or not, and "meta data", which is information about where to get information about something, or information on where you can contact given parties for possible collaboration. Operational data is not necessarily security incident related, "event data" concerns everything that happens in a given system; events are continuous and incidents represent the anomalies.

Trust is important in cooperative relationships because it reduces transaction costs in cooperation and information sharing; trust introduces sociability and deference in subjects (Kramer[27]), increases confidence and security in the relationship, and promotes open, substantive and influential information exchange (Larzelere and Huston[32]). As stated by Pardo et al.[33] "research has shown the importance of trust and trust building for cross-boundary information

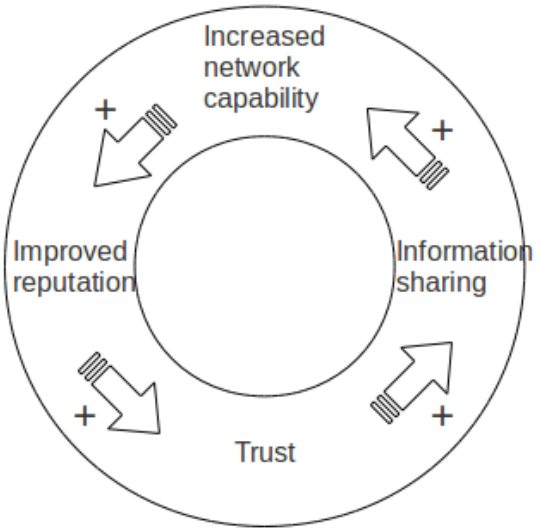

Figure 3: Trust and information sharing in an positive feedback loop.

sharing initiatives, enabling good communication and collaboration among participating agencies". Zand[34] also states that "trust has been found to be an effective means to improve communication and information sharing among group members". This is not only the case between individuals, but also between organizations (Smith and Barclay[35]). This is supported in the 1999 study by Kerr et al.[36], where they found a clear correlation between trust and information disclosure, see Figure 3.

According to Butler[37], sharing of information is caused by initial trust expectations and information quantity shared, partially mediated the relationship between trust expectations and climate of trust. Two important observations from Mandy Messenger[38] is that "participants' expectations can change over time, and develop through personal experience" and "successful past collaborations can reduce the ambiguity associated with perspective information sharing", which are the equivalents of "personal" and "experience-based" trust, respectively. The Information Assurance Advisory council also recognizes the correlation: "a better understanding of risk could facilitate information sharing"[39].

Yuki et al.[28] discuss not only cultural differences, more specific Americans vs. Japanese, in trust level, but the effect this has on information sharing both within cultural homogeneity, and across borders.

Rousseau et al.[18] emphasizes that although trust enables cooperative behavior, cooperation is not the same as trust. One must facilitate for cooperation, but mere cooperation can be forced, whereas trust can not.

2.3 Trust networks

Electronic trust networks is not a new thing, there were communities of peers already in the 1980's in USENET groups, as well as other interest groups on the Internet (Khambatti et al.[40]).

The personal trust was variable, but the trust in competence could be relatively high. Rousseau et al.[18] claim there at some point has been a shift from institutional trust to individual and network-based trust. There are probably cultural variations in this area, as we will discuss later.

According to Levin et al.[41], social interaction will lead to exchange of more resources and knowledge, and a major advantage is sharing and collaboration.

A trust network can be anything from a family to a group of friends, a workplace, inter-organizational collaborations or as most of the networks we look closer at: international trust networks (Jianghe Niu[30]). Networks can be consciously formed, or they can emerge from practices, they can be managed or not, formal or informal, voluntary or mandatory (Ruuska and Vartiainen[42]).

Several information security initiatives, like CEPS' Task force for Critical Information Infrastructure Protection[43], have focused on building networks to exchange information security information to initiate fruitful discussions and share general content, contact information, warnings and notifications, and such a network can be one method of addressing organizational and cultural barriers, and overcoming the frictions of distance (Kimble et al.[44]).

Trust groups where the members have little obvious similarities, like culture, gender or social position, should make sure the members are similar in key matters (Bowles and Gintis[45]), this can for example be by agreeing on a common goal, method or vision. They go on to discuss that deciding which traits that are important to establish trust is something that should be attempted done for the individual network, as this differs greatly. Brewer[46] claims that just being a fellow group member is a good start; individuals tend to attribute positive characteristics such as honesty, cooperativeness and trustworthiness to other group members.

To be able to go from single trust relationships to trust networks, you build on a form of transitivity, as described by Abdul-Rahman and Hailes[14]. Catherine trusts Greg, so if Greg recommends Elizabeth, Catherine also trusts Elizabeth. In these networks this is called vetting. Vetting shortends the transitive trust links, and can be seen as experience-based trust by proxy. However, one recommendation, even if in the right context, does not constitute a robust link, hence many networks demand vetting from several existing members to make the network more robust, Doney et al.[12], see Figure 4. This will make the network more resistant to single failures or attacks. All the existing trust networks we have examined have a requirement of at least two vetting recommendations, see Figure 5.

The value of the recommendations depends on the policy of the network, on the individual member and the strength of the link between the members, and also on the reputation of the vetting party, Abdul-Rahman and Hailes[14]. The more trustworthy the vetting is, the stronger the tie is to the network, and according to Levin et al.[41] stronger ties lead to the exchange of more useful knowledge. The vetting process is not without risk for the recommender, because her reputation is at stake if the recommended party is dishonest or "can not deliver what he promises", Khambatti et al.[40]. Some of the trust in the network will be role-based; the role occupant is expected to fulfill her fiduciary responsibilities associated with the role, Barber[47], which would be closely related to trust in the competence of the individual. One interesting aspect is that several trust networks are built on team membership. Each security team or group has one or more representatives in the network. Whether the network really trusts the whole

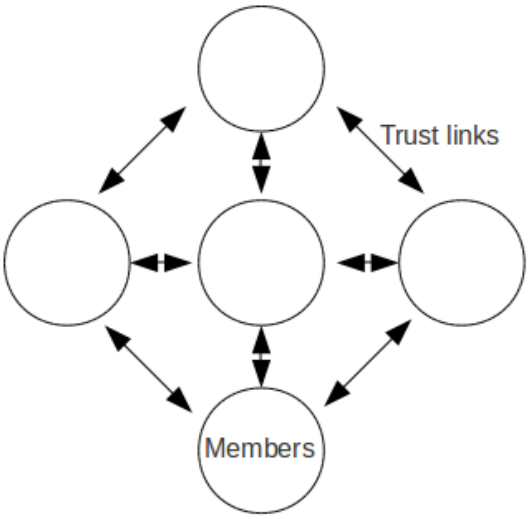

Figure 4: A robust network where all members know each other, a full mesh.

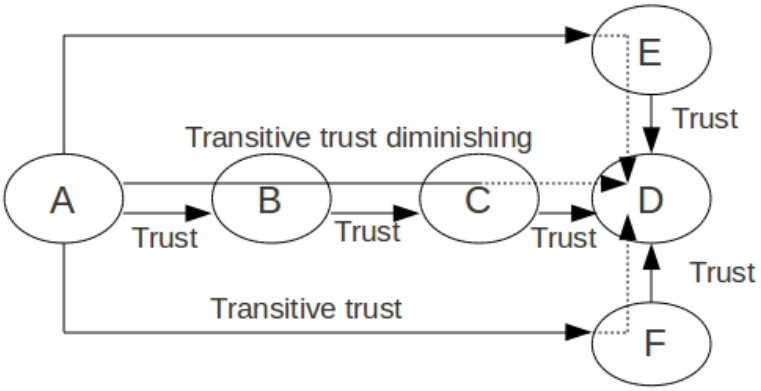

Figure 5: Vetting shortens the trust distance, and eliminates long, transitive links.

team is doubtful, as degree of competence and otherwise trustworthiness will vary, Jarvenpaa et al.[25].

Khambatti et al.[40] also point out that one can see "popularity" of a member as a background for new network links forming. We believe these would primarily concern links in the already existing networks. Although increasing robustness in the network, popularity is not something we consider further.

The creation of new links, and the strengthening of existing links in existing networks is nevertheless important. In the beginning the network is just a "validator" of trust for new members (Kramer[27]), but after a while it becomes an arena in which "trusting relations are enacted and organizational interaction serves as its own reward" (Fine and Holyfield[48]). Following the model of Jøsang et al.[3], people in trust networks should be encouraged to strengthen the network robustness, by making new connections within the network or strengthening existing links. In practice this would mean keeping up activity, social activity even, or initiating collaborations with members of the network with whom you have not had previous collaboration with.

A trust network dies or dissolves as soon as doubt becomes too great about the trustworthiness of other members, Kramer[27], the same happens if the competence level sinks too low. A curiosity here is whether "negative recommendations" carry the same weight as positive. Mathematically they do as discussed by Jøsang et al. but not in real networks. Members are more reluctant to tear down a relationship on account of one "negative recommendation" than to build one on account of a positive one (Rousseau et al.[18]). This may be counterintuitive as there is consensus that trust is more easily torn down than built up, see Loss et al.[29] and the interviews in Chapter 4. But the negative recommendation comes from a third party, and as observed by Kramer: third parties "tend to make only partial disclosures about others", "communicate incomplete and skewed accounts" and may tend to communicate what they think you want to hear (Kramer[27]). If this is the case, the scepticism should be towards forming a bond just on account of one single third party positive recommendation, not towards not tearing down a bond on account of one single negative recommendation.

The best one can hope for from an external third party is that they are trusted to be neutral[27], which may be said to be the case for key signing authorities. A PGP signed network shall, if conducted properly, be a trust network with visible vetting if the signed keys are uploaded to a key server. PGP networks are fairly robust networks, Guardiola et al.[49].

A visibility in vetting could increase network transparency (Abdul-Rahman and Hailes[14]), and increase trust. Intuitively this is true, because if it is easier to see who trusts a person it is easier to make a trust decision.

2.4 Summary of aspects of trust and trust networks

Trust is a group phenomenon, but most trust is personal. The interviewees used the terms "real trust" and "personal trust". By "real" or "personal" trust, most people mean "experience-based" trust. This coincides with the terms history-based trust and relational trust used in the literature. Transitive trust is experience-based trust via proxy.

Organizational or system based trust is a group phenomenon that some argue evolve when experience-based trust reaches a certain level, or there is enough trust bandwidth (experience).

This is related to rule-based trust. The claim that this kind of trust represents trust at a higher level can be explained merely by the fact that if the normal state is one of high personal experience-based trust, this is not actively managed on a daily basis, instead trust is put in the system. An example would be if a society and a government that is well trusted creates rules or laws, these rules and laws will be trusted. This kind of trust is heavily influenced by cultural factors, as some cultures in general have a stronger system-based trust.

We have not gone deep into organizational trust in this thesis, we leave it for future research. We consider technical trust (e.g. PGP), and deterrence based trust as being out of the scope of the thesis.

Keeping these factors in mind, we organize some aspects of trust networks in the following table:

	Aspect	**Positive**	**Negative**
Organizational	Increased group size	Increased available competence and data	Difficult to trust the network enough to share data
	Hierarchical networks	Smaller top level group	The vertical trust must be even more solid as there is participation by representation
	Smaller focus-networks	Smaller top level group, less diversity in group	Can loose focus or overstep mandate if not guided
Activities	Sharing of incident data	Enables a knowledgeable member to better prepare for incidents	Leaves sharing party vulnerable, especially reputation-wise
	Sharing of expertise	Potentially gives a larger joint knowledge base, the competence of the individual member increases	It can put a strain on particularly knowledgeable members as they become role models, It can give unfair competitive advantages in commercial settings if not properly regulated.
	Exercises	Enables a preparation of a framework or information flow strucure	Can give false sense of security. Can take up much valuable time.
Group characteristics	Cultural diversity	Enables understanding of a larger variety of adversaries	Misunderstandings or language barriers can lead to diminished trust
	Law enforcement participation	Increases leverage and possible actions in cyber crime cases	Law enforcement may have to report non-incident-related illegal data shared

3 Review of trust network research

In this chapter we go through relevant related work in our main areas of interest: networks size and -types, network governance and dynamics, incentives to become trust network members, the importance of network activity, the effects of exercises, culture, gender and other barriers to trust and information sharing. We round up with looking at the importance of frameworks, rules and guidelines.

3.1 Network size

Intuitively, we know that network-size will have an impact on trust. As a group size increases, it becomes increasingly difficult to know all group members personally, which to many is a prerequisite to "real trust" (experience-based trust).

Shaw's article on group dynamics[10], however old, is still considered a corner stone in the field. He discusses how size is a "determinant of the types of structures that will develop in a group", how smaller groups are more effective and includes members in a tighter fashion.

The smaller groups have a higher degree of member participation, and higher activity level in general, which in turn is likely to increase group trust (see p. 16 and Fig. 3).

E.J. Thomas[50] also concluded in his study that "in small groups there were greater role consensus and higher ethical commitment", hence a better breeding ground for trust relationships.

Brewer and Kramer[51] conclude in their study on choice behavior in social dilemmas that some harmful effects of increased group size are: decrease in incentive associated with cooperating in the group, de-individualization, free-riding and diffusion of responsibility. We discuss these claims in detail below.

The building of trust in small "communities of practice" (see p.22) where people know each other personally is explored by Loss et al.[29], along with discussions on mechanisms to remediate the fallen trust level in larger organizations.

Jianghe Niu's study from 2006 on trust circles in Canada and China concludes that the positive effects of trust in a trust circle diminishes as the group size increases[30]. She examines the correlation between the trust circle size, the nature of the trust in the circle and the difference in information type willingly shared as "different risk levels are associated with different circle sizes". She also concludes that limits of trust circle sizes in China and Canada differ, depending on circle composition, type of information and whether the information is negative or positive. These can be important results to cultural considerations.

Literature clearly supports the claim that there is a limit to trust network size, but we also want to look at the findings on the dependency between size, information type and type of trust and see if there are countermeasures that can increase or govern trust to facilitate information sharing. These problems were also discussed with the interviewees.

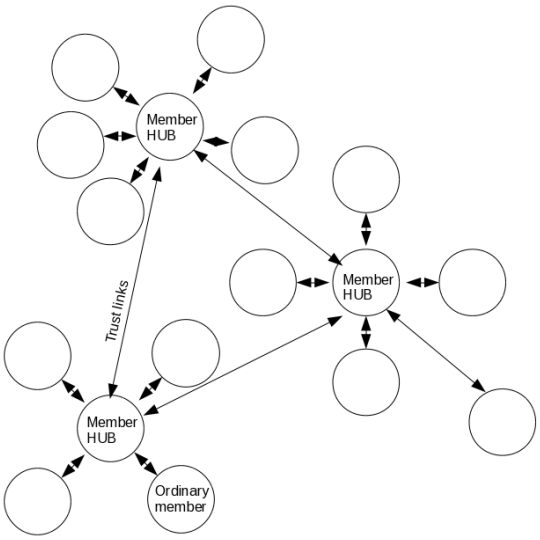

Figure 6: Scale free trust network with (human) hubs.

3.2 Network types – and structures

One way of altering the network size is to restructure the network, therefore we look at some network structures, and existing network types.

3.2.1 Theoretical networks

Basic network theory, see Audestad[52], also applies to trust networks. We do not consider random networks as trust networks are not made up of random actors; individuals or teams consciously joins a trust network. Links within a network can form semi-randomly. For instance may a security incident bring two parties together that had no direct trust relationship before. It is only semi-random because the parties have to willingly cooperate. The scale-free network is perhaps the most common structure in the security community today, see Figure 6.

Some nodes are highly connected (hubs) and the more nodes that are highly connected, the more robust the network becomes. The nodes are either individuals, or security teams if the network membership is team based. The hubs would constitute well connected people in the network, likely to be active and competent.

3.2.2 Smaller groups within the larger groups

Small groups tend to form dynamically within (too) large networks. Shaw[10] discusses the forming of smaller groups within bigger groups to facilitate more narrow specifications in process development and increase the degree of task orientation.

Two types of such smaller existing networks are SIGs (Special Interest Groups) and Communities of Practice (CoPs). SIGs have been defined as small networks working on specific areas, being technological or not, but with a clear goal of having a certain product as an outcome. CoPs are originally defined by Lave and Wenger[53] as “a set of relations among persons, activity and the world, over time and in relation with other tangential and overlapping communities of

practice" and by Wenger and Snyder[54] described as "groups of people informally bound together by shared expertise or passion for a joint enterprise – engineers engaged in deep-water drilling for example, consultants who specialize in strategic marketing, or front line managers in charge of check processing at a large commercial bank". They also point out that these can stretch across borders, national or organizational. Brown and Grey[55] used in the term "peers in the execution of real work held together by a common sense of purpose" about these CoPs.

The case study done by Ruuska and Vartiainen[42] builds on the work of Lave, Wenger and Snyder[53, 54], but takes the discussion further towards facilitating information and knowledge sharing. They explore networks from the small informal networks and "hallways of learning" to networks that are designed for a specific purpose like crisis handling networks and trust networks. They also dig into three dimensions of CoPs:

- mutual engagement (activity and communication)
- the community as a joint enterprise (common goals)
- shared repertoire (common professional reference background, vocabulary etc).

They discuss the degree of formality in CoPs/SIGs, organizational boundaries and competence diversity in such groups.

There is often a low degree of formality in such groups, and they can function well across both organizational and national borders as long as the "three dimensions" are there and well functioning, which is promising for the building of trust networks.

The SIGs/COPs can be initiated by the organization, or the larger network, or it can be initiated by individuals wanting to create a common interest group, as shown by McDermott and O'Dell[56].

Loss et al.[29, 57] examine the differences between larger organizations, like trust networks, and smaller, specialized networks like CoPs or SIGs, and investigates whether the small networks can "promote the trust building among members taking part in the larger environment", and how also the larger network can support the smaller, more focused networks. Wolf and Kazi[58] also believe that these kinds of networks can be the basis for not only a hierarchical flow of information and knowledge up into the larger network, but also a more widespread flow through the larger network. This would lead to a coalitional network structure, see Figure 7.

Gelfand et al.[59] stress the advantages of utilizing existing structures in organizations to build a trust network, as the values in established structures often are stable. They have also examined some implications of utilizing culture specific society structures as building blocks for trust networks. It can be argued that this is how OIC-CERT or EGC have been built, see page 10.

3.2.3 Hierarchical structures

Another way of organizing trust networks or information sharing activities is by creating a hierarchical structure under each person in the network,- a delegate model where all communication into a network goes through a representative or delegate, a participation through representation, see Figure 8.

Shaw[10] mentions a hierarchical model as a possibility to keep the group size down, but he does not dive deep into possible dynamics in such delegate models.

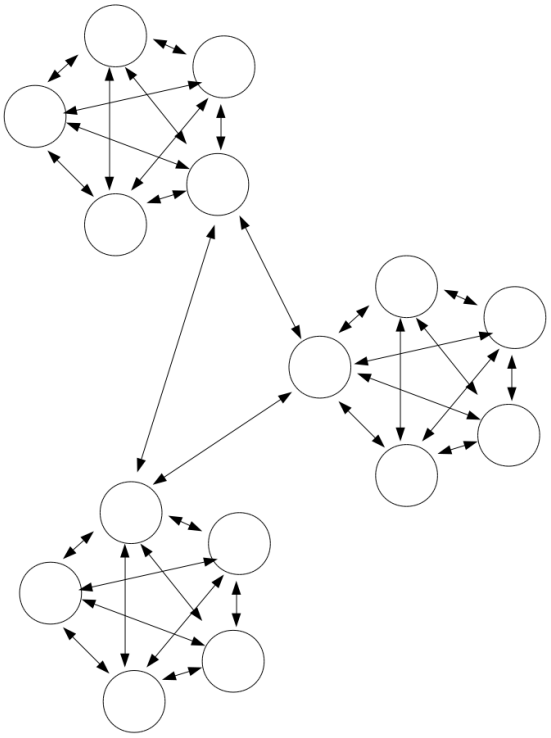

Figure 7: Coalisional network

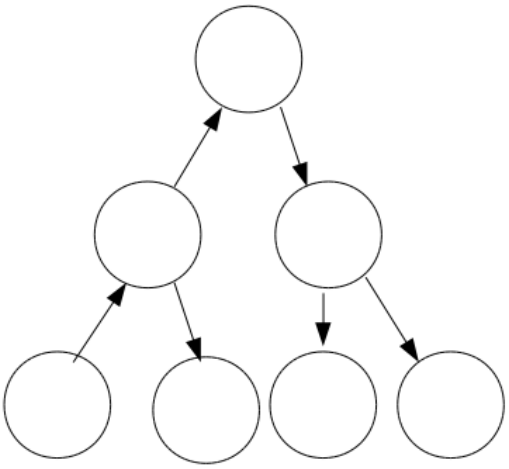

Figure 8: Hierarchical network

J.A. Wall[60] brings up the complicated issue of constituent trust. Not only must the representative assess delicate trust and communication bonds, but also handle the relationship with the community. If the delegate is to function properly in the network she needs to have the trust and cooperation of the constituency being represented. The study shows that not only does the representative need constituency trust to ensure flow of information, but the delegate's bargaining abilities seem to be positively correlated to constituent trust. However, the lack of bargaining skills could be the cause of the lack of trust, and not the other way around, a possibility that is not explored in this research. If an individual has a lack of external bargaining skills, and this is rooted in a lack of competence, integrity or even communication skills, this can quickly lead to a drop in internal trust level in the constituency. The perception of a distrusted representative is also disruptive for the communication between the representative and the other representatives in the network [60]. Mayer et al. claim there can be information sharing without trust, especially if one person/organization has substantial power over the other [16]. We do not look into these forms of cooperation any further as our focus is on trust based information sharing.

Bowles and Gintis shed light on the possibility of opposing values in the constituency and in the network [45], making the representative's role difficult, leaving her with difficult negotiations both on the "inside" and "outside".

Another issue that might arise in a delegate model is the need for the individual or the individual organization to receive credit when credit is due. McDermott an O'Dell mention this [56], and this should not be taken lightly as the lack of credit for work or competence leads to diminished effort and results in less trust hence less information sharing.

How well a delegate model functions is also affected by cultural elements, as we will discuss below.

3.3 Network dynamics and -governance

Trust in a network replaces control in many aspects, as discussed by both Kasper-Fuehrera and Ashkanasy[61] and Rosseau et al.[18], which leaves governance of trust networks slightly different than governance of companies. But the dynamics and steering of a group with trust based ties is delicate. Here we look at leadership issues and trust level fluctuations in such networks.

3.3.1 Management

The leader or leaders of a trust network can be appointed by the network or it can be on a volunteer basis, maybe by election if several wish to be in this position. A key attribute is that they have the network's trust, or else any attempt to lead or govern the network will fail. As Klijn[62] postulates; "networks are vehicles to create trust and trust creates governance advantages". Shaw claims that as opposed to emergent leaders, appointed leaders, by election or not, tend to be less authoritarian [10]. This may be so, but this is clearly context- as well as cultural dependent; some cultures tend to have highly authoritarian leaders, even if appointed.

Accepting responsibility for the group and being highly motivated are important attributes in a leader, Shaw[10]. Directive leaders were favored in the same study.

Patrick Kenis[63] discusses the need for network governance to coordinate a potential heterogeneous group, to give direction of "who is in charge" and to avoid a situation where all must

trust all. He describes three governance models: “Shared governance”, “Lead organization” and “Network Administrative Organization”, where shared governance groups require very high trust density, hence will not grow large. Lead organization has low density of trust and is therefore not suitable for the kind of information sharing we are looking at and the latter is the model that allows more than a moderate member number, and therefore will be the model of choice, see Figure 9.

Jarvenpaa et al.[25] conducted a study with high and low trust teams, and the high trust teams had rotating leadership. Elahee et al.[31] discuss rotating leadership vs. the advantages of having the same person as leader over time, creating stability and familiarity.

Jarvenpaa et al.[25] also explore elements of group efficiency enhancements like goal clarity, time management, group feedback, group role specifications and interaction frequency, all of which could likely improve with the aid of good governance.

Klijn[62] highlights the importance of managing content and managing interactions to keep a high activity level, and sustain existing organizational arrangements.

3.3.2 Trust level fluctuations

However important a leader, the network members and the trust is what constitutes the network. The trust level itself is dynamic, which is an important aspect to take into consideration. The trust level in a group can be disrupted by a breach of confidence, or by a simple thing like an individual’s change of employment situation or a new person being brought into the group. Also; because “risk and interdependence are necessary conditions for trust, variations in these factors over the course of a relationship between parties can alter both the level and, potentially, the form that trust takes” (Rousseau et al.[18]). They further define three phases of trust; building, maintenance and dissolution, and further discusses the acceptance of trust as a dynamic phenomenon.

Msanjila and Afsarmanesh[15] discuss trust level metrics and how to determine, establish and validate the preferred trust level in an organization, and Jianghe Niu[30] explains how the context, in which the trust exists, creates natural dynamic level.

Shaw[10] discusses possible disruptive effects of newcomers in groups, but also that a newcomer can be perceived as resource person, and Scott Williams’ article[64] on building trust presents a set of recommendations on re-building trust. This is also discussed by Doney et al.[12], who also go through how “behavioral anomaly may destroy trust based on predictability”, an important factor being the nature of the trust, and the “richness of the history”. This is analogous to Rousseau et al.’s definition of “trust bandwidth” and trust relationship as “shared identity”. A high “trust bandwidth” would be analogous to experience-based trust formed from substantial experience. If a trust relationship is based on a long term, high activity relationship (richness of history), and the parties have a good understanding of the other, hence the ability to predict the other’s actions (shared identity), we consider them to have a high trust bandwidth.

Kramer[27] observes that negative information is perceived as more credible than positive information, and that destroying trust is quickly done whereas re-building is a slow process. He also attributes network trust level decrease to individuals’ tendency to overgeneralize. Kramer’s finding is in opposition to Rousseau et al.[18] mentioned earlier, whose findings were that people

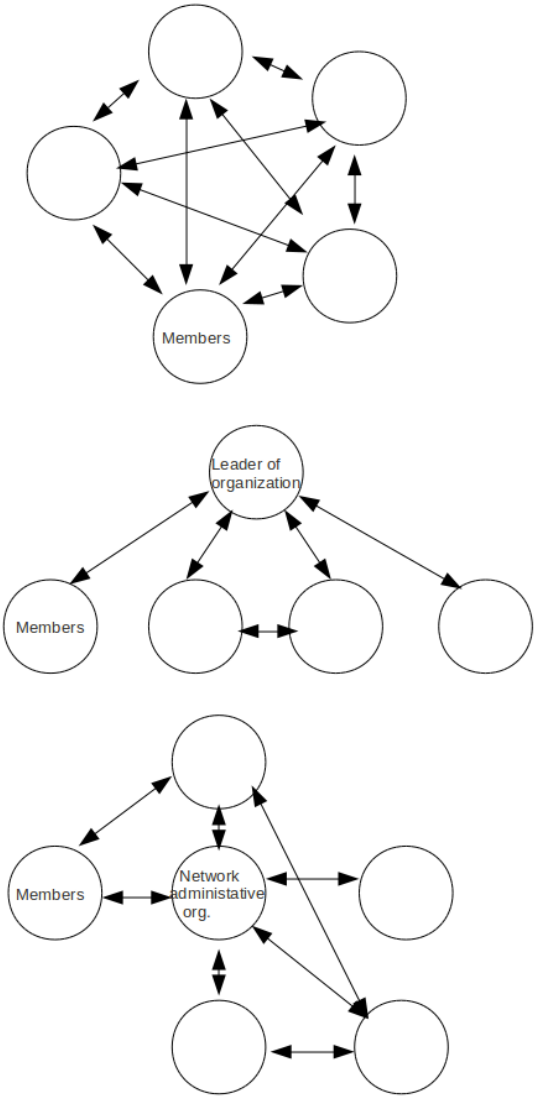

Figure 9: Kenis' organizational models[63]. From top to bottom: the self-governance model, the lead organization and the network administrative organization. The latter model is the most relevant for our setting.

were reluctant to tear down a trust bond on the basis of one single negative recommendation. This can be due to the tie strength in the trust bonds being higher in the latter research.

Both Williams[64] and Kim et al.[65] stress the importance of apology and admission following a breach of trust to restore the desired trust level, as "expression of regret signals an intention to avoid similar violations in the future". Williams claims a transparent process to be a better choice to reassure the community, hence heighten the trust level. Rousseau et al.[18] also claim that a breach of trust is a symptom of a problem that should be examined more closely, and suggests possible categories of causes in a multi-level trust model. The breach of trust as a result of larger, underlying problems would likely be especially important in intra-organizational networks, as these networks are easier to explore. This is a factor that would be interesting to keep in mind in dealing with breaches in inter-organizational and international trust networks as well.

Kim et al. present results that indicate that low perceived competence or integrity is disruptive to the networks ability to restore trust level in the aftermath of a breach of confidence.

Shaw[10] advocates clear and visible consequences of trust breaches, a practice that is common, but not undisputed as we will see later.

The trust group composition is essential to all phases of trust and trust dynamics. Jianghe Niu[30] presents several aspects of trust circle composition, the cultural variations in the composition and the impact of the nature of the information to be shared. Cultural aspects in composition is also considered by Yuki et al.[28], including possible the positive impact of different cultures in the same network.

An entirely different aspect of group composition is the possible conflict of interest of participating parties, the effect this may have on the perceived trust in the network and how this affects information sharing. Some possible actors being regulatory authorities, as described in Moberg et al.[66] and law enforcement, depending on the domestic laws in the respective countries.

3.4 Activity and network value

The value of the network itself is closely related to network activity, and is of course directly correlated to the incentives of joining a network.

3.4.1 Incentives for trust network participation

There have to be incentives for groups or individuals to join a trust network or to share information within the network. The incentives differ slightly depending on the role of the individual asked, e.g. whether the person is a manager or an engineer.

The ENISA study[67] looks closely at incentives for participating in sharing, where the two most notable reasons are "economic incentives stemming from cost savings" and "incentives stemming from the quality, value and use of information shared", where cost savings can stem from "quicker reaction to threats, vulnerabilities and attacks, or from anticipating network failures".

Gal-Or and Ghose[68] also identify cost savings as an incentive, and increased efficiency due to joint effort on development or incident handling. Loss et al.[29] highlight increased diversity in experience-based knowledge as an important incentive. Ruuska and Vartiainen[42] also dis-

cuss how to prevent the reinvention of the wheel by sharing incident information. Klijn[62] discusses innovation as a possible outcome of sharing.

Both Kolekofski & Heminger[69] and Dermott & O'Dell[56] point out that sharing information can be a symbol of power. This can be either because sharing reflects competence and resources, or because it flags a generous and giving organization that can "afford" to spend resources on helping others.

The ENISA study consider "incentives stemming from the reputational benefits of participation" to of lesser importance, a statement that would likely be colored by the nature of the interviewees roles. Both Kramer[27] and ENISA mention trusted relations and interaction in the network as a reward and an incentive in itself.

3.4.2 Network activity

The sharing of information in trust networks matters. Not only does sharing matter as means to an end, but showing trust by sharing breeds trust, as discussed earlier. Fuehrera et al.[61] plainly concludes that activity breeds trust. The opposite is also true, as pointed out by Williams[64]: "we tend to withhold information from people who seem to resist opening up to us".

Doney et al.[12] point out that the perception of intent is important, and that sharing information helps establishing trust in intent, and Kramer[27] claims that "absence of reciprocity in exchange relations erodes trust", or as Williams[64] state, "if you do not do anything, how will your peers experience your trustworthiness?"

Gal-Or and Ghose[68] also bring up the consideration a disruptive affects of "free-riders" in information sharing communities, and the need to consider possible shift in competition advantage amongst sharing members, and Doney et al. stress the importance of the quality of the information shared; it must be correct and timely. Kolekovski and Heminger[69] advocate the same view. Data relevance and timeliness as important factors is backed in the ENISA survey[67], and in addition they found it important for the data to be at a suitable level (operational, tactical and sensitivity wise). As this is an element that was brought up by several interviewees as well, it will be further explored.

The ENISA study also brings up "free-riders", but suggests a strategy to look into cases more closely as it may be caused by e.g. lack of funds, competence or simply lack of access to data of equal "value".

In skewed sharing relationships, the party of higher competence or with better conditions for sharing may still share and can gain benefits from this, but being such a "role model" may also be a heavy burden to carry, as supported by Constant et al. [70], although they argue sharing may produce significant personal benefits to the information provider because it permits self-expression and demonstrates self-consistency.

Msanjila and Afsarmanesh[19] discuss reputation as a trust measure, where a "role model" would typically have a better reputation, being recommended by more peers, and Khambatti et al.[40] present possible ways to give numerical weights to such trust attributes as reputation, as do Falcone and Castelfranchi[71]. We do not discuss numerical weighing further.

Jianghe Niu[30] suggests that it is important the "role models" or the strong parties in sharing networks, share their "negative incidents", as it increases credibility. Sharing this kind of inform-

ation, the sharer appears more open and vulnerable to the other trusted parties, hence more trustworthy. The more serious a "secret" one party shares, the more they seem committed to the trust relationship. As mentioned elsewhere, there is a limit; it all has to be within the "right" sensitivity level. The ENISA study also mentions "access to human resources", like the aforementioned "role models" as a possible reason for participating in trust networks. This is not rated highly in the ENISA study, which might be due to the nature of the interviewees, which are likely representatives of "role models" themselves and hence have less need for external competency.

3.4.3 Incidents and Exercises

Real incident data and collaboration has been proven to improve trusted information sharing, at least for a limited time period. This is described in the ENISA report [67] and was also seen in the attacks on Estonian and Georgian government, and the subsequent flow of information in several international networks. This phenomenon of increased trust between what is perceived as fellow confidants is a common effect of serious incidents, not only of cyber incidents.

The use of exercises as incidents to gain the same type of experience is controversial as to the efficiency of such exercises, but the reports from e.g. Cyber Defense Exercise (CDE) [72, 39] and Cyber Europe [73] are positive to the effects of the exercises on trust and information structure awareness.

Conklin and White[74] recommend exercises to "provide insight into operations and provide the participants an opportunity to determine their strengths and weaknesses", and claim the exercises provide important findings. Important to note is that this is exercise vs. reading a report, not vs. working on a real incident.

Jarvenpaa et al.[25] stress the importance of deploying trust building exercises in virtual organizations, on the other hand, in their field study the exercises seem to have the effect that the parties gained knowledge about one another, but the network trust level was not significantly elevated. This might be due to the fact that (experience-based) trust building takes time under normal circumstances. They also discuss that the fact that if you behave well throughout the exercise, this might have a positive effect on trust as you appear to be a "team player".

3.5 Barriers to trust and information sharing

There are barriers to trusted information sharing that are hard to remediate, like for instance breach of trust with perceived ill intent. Lack of trust, poor leadership or missing structures to support cooperation are all determinants that are barriers to information sharing initiatives, as discussed by Pardo et al.[33]. The ENISA study[67] also mentions poor management as well as poor quality of information, type of participants, legal matters and group size. They are all treated separately in this thesis. Fear of reputational risks or leaks are also mentioned, we attribute this to a general lack of trust. A barrier to information sharing is the difficulty of finding the appropriate level of sharing and the appropriate level of information to share. As already mentioned, Jarvenpaa et al.[25] point out that the ones that are too promiscuous with their information can easily been seen as either careless, naive or incompetent.

Rumors and suspicions in general, are barriers to trust, and both Kramer[27] and ENISA[67] mention uncertainty in regards of the government's intent as a potential barrier. Competitive

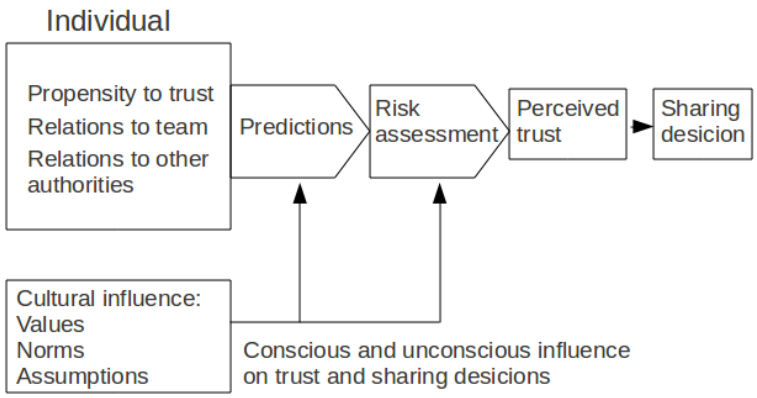

Figure 10: Cultural influences on the sharing decision

issues between companies can certainly be an issue, and the ENISA study brings up rivalry as a barrier.

Kolekofski and Heminger[69] present some interesting and not widely discussed results: that some do not share because they either see the information as potentially uninteresting, or are unsure how to interpret their own data, and do not wish to be perceived as incompetent. This can even be one of the reasons bilateral sharing relationships are formed. In these smaller networks, it is easier to risk "losing face". This fear can be one or the reasons some network partners appear silent and inactive.

International law and national borders can be a barrier in itself (noted in the 2010 ENISA study[67]), and the differences between countries can be "deeply rooted in ancient tradition between the state and civil society", Lane[75], and as Bachmann[26] points out; this difference can be large even between countries like England and Germany. A barrier to both trust and information sharing in networks is culture, which we will discuss separately.

3.5.1 Culture

In trust networks that are created to exchange incident information and possibly spawn virtual incident response teams, cultural elements affects almost every step in the trust building and in the enabling of information exchange. Culture, in this context, is national culture, not for example organizational culture. It is the shared values, beliefs and practices of a group of people (McDermott and O'Dell[56]). They have common morals, attitudes and see their peers as "similar", making the internal network homogeneous and less complicated (Alesina and La Ferrara[76]). See Figure 10.

Shared perception of justice is important to make participants not only follow common rules, but also believe in the means and goals in a trust network. This is especially important if the cultural distance is high (Yadong Luo[77]). Gelfand et al.[59] discuss cultural differences in negotiations and in team dynamics – e.g. how members of different cultural backgrounds may react differently to member replacements. They also discuss variances in effective leadership qualities across cultural borders and performance and communication in heterogeneous, multi-

national networks.

Trust relies on a person behaving as expected, hence one must know what to expect. Bachmann[26] explains how German and British cultural history can differ enough to make trust networks for information sharing complicated, this due to difference in basic trading philosophy.

As Kramer[27] points out, a rule-based trust is not a trust built on "fear of consequences, but on a shared understanding regarding the system of rules regarding appropriate behavior". This stresses the need to shape a fellow platform of understanding.

Masaki Yuki et al.[28] point out that the trust level in different contexts is different in Japanese and American groups. Jianghe Niu[30] has looked at Chinese vs. Canadian groups, finding that the attributes that increase perceived trustworthiness are not the same in different cultures. Attributes like age, education, personal reputation, position in a company, or personalized knowledge can potentially affect trustworthiness (Kramer[27]). Jianghe Niu also discusses how "shame" and fear of loss of reputation are also factors that are more accentuated in some cultures than others. This will also skew the willingness to share negative vs. positive information. Both Jianghe Niu and Doney et al.[12] discuss how relation to authorities, like a boss, father, older sibling etc. is important to consider when forming a robust trust network.

Some collectivistic cultures seem to favor individuals from the same culture in a larger degree than individualistic cultures do, Elahee et al.[31], in that study the subjects were from North and Central America. Jianghe Niu's findings suggest some cultures seem to be more "trusting" than others.

Pardo et al.[33] stress the importance of having respect for the autonomy of participating organizations and the importance of clear roles and responsibilities to avoid misunderstandings.

Kim et al.[65] discuss how, considering international culture differences, the standard for trust repair in a network is best handled, by denials, by exclusion of individual perpetrators, by apologies and with or without a lengthy explanation of the reasons why.

To be able to facilitate a cross-cultural network, you would have to read the cultures involved, which is complicated because culture is not necessarily a conscious behavioral pattern and as the culture is so interwoven with the individuals' personalities, one would have to take care not to tread on people's toes (McDermott and Carla O'Dell[56]).

Kimble et al.[44] claim that the cultural diversity in a network increase the need to meet face to face, although Jianghe Niu[30] finds in her Canadian-Chinese study that the level of reassurance of face-to-face meetings differ from culture to culture. Zaheer et al.[78] support the importance of microlevel relationships to enhance macro level trust: "broader forms of trust can be influenced by microlevel arrangements – in particular, how individuals representing each firm relate to each other". This supports the importance of working on a micro-level cultural understanding to support the operation of the larger network.

Msanjila et al.[19] postulate that in organizations of several cultures that are not familiar with each other, the importance of "social trust" is higher, which would account for the aforementioned "organizational trust".

The need to work together in a trust network has a contextual limit, the goal of the network is to share some kind of incident data. There is no need for "full cultural understanding", as most aspects of a culture will never be relevant. Tsai and Ghoshal[79] found support for their

hypothesis that sharing the vision of the network is correlated with perceived trustworthiness. Jianghe Niu[30] points out that trust circle composition is dependent on context, perceived risk, and show significant cultural variations.

3.5.2 Gender

Many, of both genders, expect females to react differently in many trust situations. However, there are also contradictory studies to this, Kramer[27]. We consider this beyond the scope of this thesis, and believe that in highly specialized environments like information security professionals, gender does not alter situations significantly.

Another issue is whether representatives that have roots in certain cultures would question the competence, or challenge the authority of a representative based on gender. This may be the case, but all the cultures considered in this thesis are masculine. This would exclude the discussion of the feminine or the masculine as the "stronger" party, we will however include gender as a possible barrier in the discussions.

3.6 Frameworks

Since many professionals, including some of the interviewees, strongly advocate the use of frameworks and emphasize the importance of rules and guidelines, we consider some important work done in these areas.

Although "virtuality requires trust to make it work, technology alone is not enough", Kimble et al.[44], there are a number or existing frameworks for trusted information sharing and proposed trust metrics/values that can support trusted information sharing. We will not be considering any proposed trust metric standards in this thesis.

The scope of the ITU-X.Cybex[1] framework nicely sums up what a framework covers:

- structuring cyber security information for exchange purposes
- identifying and discovering cybers ecurity information and entities
- requesting and responding with cyber security information
- exchanging cyber security information
- enabling assured cyber security information exchange

Some other examples of frameworks are: the recommendations from the British ministry of justice[80], British health care data sharing guides[81], the ENISA supported project AREKI and the Messaging Standard for Sharing Security information: MS3i. ENISA has published a feasibility study for a European Information sharing and Alerting System, EISAS, which concluded in FISHA, Framework for Information Sharing and Alerting[2], and also published a set of best practices[82].

If the network is trusted, the use of appropriate frameworks can remediate uncertainties of data leakage due to technological issues or inappropriately exposed information. Trusting the framework is however dangerous as technical innovation works both on the good and the bad

side, and even a secure technical environment can develop vulnerabilities, and will be attempted exploited, Msanjila and Afsarmanesh[19].

Kimble et al.[44] discuss virtual teams/communities of practice and the usefulness of frameworks: “theoretical frameworks are needed to understand the different aspects of virtual team working and to guide their development in real organizational settings” and the result of the ENISA study[67] indicate that the participants in the study believe clear rules, processes and structures are important to enable information sharing.

3.7 Membership rules and guidelines

A trust network must have guidelines, rules and/or Best Practices. Whether they are written or not, they need to be clear, spoken rules if the network is anything other than a group of friends. A clear rule helps stake out the vision, and should give an idea of the context and framework. Camarinha-Matos and Afsarmanesh[83] divide the guidelines into four dimensions: structural, componential, functional and behavioral. The guidelines describe everything from possible participants and roles, to guidelines for behavior/code of conduct, mandatory rules, constraints and conditions (NDAs etc), cooperation agreements, processes and methodologies, or even human or technical resources used in the network.

When we deal with multi-cultural networks, taking for granted that everyone understand a common rule set, goal or intent without explicitly stating these is not productive, Kramer[27]. One might even consider it arrogant.

Jarvenpaa et al.[25] find in their study that the well functioning team had clear task goals, role division and specificity. This can not be obtained by rules alone but rules can function as beacons of intent. As Pardo et al.[33] formulate it: “a clear definition of roles and responsibilities helps to build trust by clarifying what each participating agency is responsible for and decreasing uncertainty about leadership, decision-making processes, and fairness among participating agencies”.

One important factor is that even if there are rules of engagement, the punitive capability in the network is not necessarily positively correlated with trust level. In their 1998 study, De Dreu et al.[5] found support for a negative correlation between high levels of punitive capability and trust. They also found high punitive capability to lead to less information sharing and also agreements of lower joint outcome.

4 Results of the interviews

In this chapter we look at the results of the interviews in light of the research questions, how the results correlate with relevant literature and what new questions emerged.

The interviewees were given an overview of the topics in advance, but not the actual questions. They were aware that the basis for the interview was their participation in trust networks and information sharing initiatives. The professionals were asked to answer the questions as individuals, not as a representative of any workplace or organization, and they were encouraged to be frank, and answer based on their own empirical observations. To obtain this, the interviews were informal, with no time limit, and the interviewees were ensured they would get the opportunity to edit the transcript before anyone else besides the interviewer had read it.

The interview guide was originally in three parts: network size, trust dynamics and barriers to trust, but as new and important questions came up, the guide was adjusted accordingly, so we have chosen to analyze the results based on the resulting interview structure, not the original one, see Appendix B. The quotes in this chapter are quotes from the interviewees.

4.1 Network size

The opinions of the interviewees were consistent with sociological studies, that size of a trust network matters, as discussed on page 21. They also stressed that trust was dependent on personal relations.

One of the interviewees said: “There certainly seems to be a size beyond which personal relations do not work, I suspect it is somewhere around 100, I think it was when we came to about 100 teams people started agonizing about why trust had gone”.

This was supported by another interviewee: “when I was still in the secretariat we noticed that when we had grown over 100 members, which is a long time ago, things started to get more difficult.” She also pointed out that any matrix structured organization would likely have a scale problem at some time, as opposed to for instance a hierarchical model. This interviewee was the first, but not the last, to mention “the beer drinking model of trust”, which of course does not mean that participants necessarily meet to drink beer, but meet in an informal situation which is a good setting for forming personal relationships.

Two of the interviewees favored the membership in smaller networks, and found the larger networks to be too big for sharing of real information: “those networks are not really operational networks, here we share for the most part meta-information, and this is not really sensitive: contacts, incident trends etc.”, “it is not an operations network, more of a trust broker, it is too big to be operational”.

One of the interviewees stressed that size was not necessarily a problem, although normally network size is inversely proportional to trust level, the fact that the network was merely a “trust broker” was fine. She said that at least you could have a network of people who probably knew someone you could trust.

This, and one interviewee's statement that "the smaller the group is the more and the better information will be shared" hints of a categorization of trust networks, whether the network is a direct trust network for information sharing or a trust broker for sharing meta-information. So we are not only looking at the quality of information shared but the type of information. Meta information is not necessarily of any less value than operational information. So if the need for personal trust in a meta network would be less, as this would be based on bringing participants together and encouraging them to form a trust bond on the outside of the organization, would these trust networks members have the need to meet in person?

Several of the interviewees were quite insistent: "These meetings serve several purposes: increase trust by actually talking to people in an informal context , exchange ideas and get an idea of what others are doing, and gauge in comparison with your own organization". "In my view, at the end of the day it's always personal trust, like it or not. At least the CERT people admit that".

This would mean that even just to recommend a contact person to someone, you need to build some trust in these contacts, and this is experience-based.

4.2 Network types

Some trust networks are created from scratch to be kept small, and others are just spawned from larger networks for different reasons - some just to work on specific problems, whether the problems are of technical or administrative nature. The larger networks can function as an enabler for these special-purpose networks. As described by an interviewee: "the large network forms a community where you meet people you decide to work with in smaller groups, a two-stage process". But the smaller groups do not have to be formed on the fly, they can exist alongside the "umbrella" organization all the way.

One of the interviewees expressed great enthusiasm over the smaller sub groups: "my suggestion would be to create sub groups within the network. This is the function of several Special Interest Groups (SIGs), which gets back behind the size threshold". She also had experience from her own country where they formed a political focus group on some particular security issues, and under this umbrella formed a small, technical group of a maximum of 12 people to get a specialist view on the problem. "This group is having superb discussions and reporting back to the legal department." The political "layer" does not even participate in the meetings, but there is a liaison - they have the same secretary for both groups". She explains that they forget what organizations they are from when they work together: "they become a group of 'techies' working on a hard problem together." So the political or "legal layer" may dictate the nature of the problem to work on, but they do not interfere with the technical side, not even as observers. They merely provide a support function that will be of help to all and ensure the reporting.

Another one of the specialists, also mentioning the possible compartmentalization of larger networks, saw the new Trusted Introducer (TI) certification scheme as compartment forming. On this another of the specialists deeply disagrees, since the certification is not meant to split up the network, but to create a goal for teams. She was mostly preoccupied by the advantages of the uniformity of smaller networks; "it is a natural cooperation like governmental CERTs. As there is cooperation in the other levels of government cooperation on CERT matters as well

is natural. The banks cooperate in ISACs, they are sort of natural partners for one another. In general, sectoral compartmentalization is a good idea..."

The European Government CERT (EGC) was mentioned: The government CERTs have their own trust network. They all see similar attacks and probing towards critical infrastructure, which is natural for them to share internally. "The network enables them to compare and baseline the network activity against the others, learn from each other and share security solutions."

The MELANI network differs significantly from the others as it is not matrix structured, and there is a party, a governing hub, that does all the formal contract work (NDAs etc), receives all the data, sanitizes it, and shares it back to the members. This can obviously work well if the hub is known and trusted, and if there are no psychological barriers. Two of the interviewees were sceptical to this structure, on the other hand, other interviewees believed it to function well.

A couple of the professionals were partial to small networks with specific focus areas, high demands, and strict vetting within the network. "The vetting means people or teams are up to a certain standard". They both agreed that the forming of most networks was a natural and dynamic process: "it is the trust that creates the network end not the other way around". They both stressed the importance of letting this dynamic process work and not interfere or force anything.

An observation is that these smaller networks, however dynamically formed, tend to have very strict vetting and written rules, but the vetting process can be informal, of the form "he's a good guy" and the rules can be a plain text document passed around. Large official trust networks are governed and more formal, but smaller and tighter networks tend to form dynamically within the larger networks.

They all agreed that sector groups for certain sectors would potentially be a good thing. There is some international work on this now but it has come surprisingly short considering the unison praise of this structure. There is a European financial ISAC, but one of the interviewees claimed it was normally not used for this kind of information sharing. This is a network for more than just information security, it is also meant for sharing technical details on solutions etc, so it might not be the appropriate channel at all for incident- and cyber security related information.

4.2.1 Hierarchical networks, delegate models

An obvious remediation to growing network sizes is a hierarchical model. Most of society is built up hierarchically, and if the information flow and internal respect is maintained, this could perhaps solve the diminishing trust in large trust networks. Bringing up the question of hierarchical trust networks with the participants however, provoked controversy. A couple of the representatives brought up the fact that someone had tried to create "EuroCERT" some 13 years ago, and that it failed entirely. The idea was according to one of the initiators that "European CERTs were supposed to report to EuroCERT, and EuroCERT would sort it out with the rest of the world", this would comply with wishes and expectations from the political arena, both the EU and local governments. Even from large companies in other parts of the world, as Prof. Dr. Bernard Hämmerli said: "they want to call Europe".

There are several potential problems with this model. First of all, as several of them pointed out: "The Internet does not know what Europe is. The perimeter of the European Internet does

not exist. Who do you phone to speak to Europe? You could of course have a 'point of contact', but no one could speak on behalf of Europe: that would not work.“ This indicates that first of all there is the issue of designing the mandate. Having a point of contact could be more acceptable than having a spokesperson. Another issue is of course the definition of Europe. The European Union is trade based, and this is not necessarily the criteria you want to use for this purpose, you might want to define Europe without an existing model in mind, and instead focus on the purpose of the point of contact. However, if the initiative was not built on existing political structures, it would most likely have to be financed by the members or sponsors.

Another obstacle in a hierarchical model is that the parties further down in the hierarchy would have to give up representation. One of the interviewees summarized this nicely “It will not work if you try to create a representing group out of the blue just for this activity. Then the institutions would want to have a representative themselves. They want to be seen, to have their brand in, stuff that has no relation to information sharing,- human vanity even. There may also be a lack of trust that this one representative will do what is best for each and every one of the constituency.” She pointed out something that is important; the wish to be seen and acknowledged. This was mentioned by several of the interviewees, and this suggests that a representation by an external party in a trust network would be insufficient for many. Another of the interviewees stated that “it is hard to give up representation, but at some point you have to say I am not the best person to contribute,” but was also eager to add that it is imperative the representative have the relevant skills. The skills of course being dependent of the mandate, and one would assume such a representative would be slightly more administrative as opposed to technical. She also suggested that the “representative” should be “humble and polite to the community” (here meaning the constituency): “if the acceptance of a delegate is forced, this will not work. Offering a meeting and collaboration is better than demanding reports”. It would take time before a representative would be trusted by a constituency, and the trust would have to be experience-based, and would have to be based on trust in the representative's expertise and benevolence.

One would think that geographical, hierarchical representation would be a fairly easy structure, but history shows otherwise. In one of the larger trust networks, there was a confusion on two accounts on which team was appropriate to represent a country. Both countries suddenly wound up having two separate teams in the network claiming to represent the country. These controversies have been resolved, but clearly show that a representative not only have to be accepted by the constituency, but also must be endorsed by the absolute top level in the domestic power pyramid.

Some of the interviewees believed a hierarchical model would function better in a sector type network[1], “it is easier to trust that the representative has the competence and will to represent each one in the constituency properly”. This would be true if the representative was skilled in the relevant sector field, but still company neutral. Another interviewee believes that this would mainly work in the event of an incident: “Under the handling of an incident there is a need for a representative to be the voice of the people working on the incident, as they may be spread across both company and country borders. The mandate and resources must however be clearly

[1] Sector networks, here meaning for example “health care”, “power companies”, “law enforcement” etc.

defined. You have to trust that this person/representative will be true to what the networks are conveying, which also means the content must not be too technical. It has been proven useful in past incidents".

However obvious the potential single point of failure in a hierarchical model might be, only one of the professionals voiced scepticism to the security of a hierarchical trust network model: "I find them unreliable and vulnerable. What if the top level is compromised? Then you have a problem. It is a good idea politically, but it would not work in the real world, or the Internet as we usually call it."

4.3 Network dynamics and -governance

Trust is a dynamic phenomenon, and even if building trust is a lengthy and complicated process, tearing the trust down is done in an instant. Like one of the interviewees said: "Trust falls by the meters and grows by the millimeters." You can have an information sharing framework, or contracts like TLP[2] or an NDA[3] - they are all no good once the trust is gone".

In some networks, like in the military model, trust is forced, and some people clearly see this form of trust as more secure. The interviewees did not believe this is the right direction: "For the stronger form of trust some believe you need the military style; you flick from an information sharing mindset to an information restriction mindset. You start thinking rather than *do I share this information* to: *do they need to have this information*. It gets more restricted and it has not been a success."

Another interviewee was clear on the nature of the leadership in trust networks: "Basically, you can not force trust. You can not have an all solitary, all powerful CEO/CIO that dictates trust, it does not work that way". They did, however stress the need for good leadership in the trust networks: "leadership should enable people to do things better, but not enforce trust or anything like that. All management and leadership should only help people do their things instead of just forcing laws and regulations onto them. But you do need good leadership."

In a trust network, if the trust for some reason has fallen, a solution to obtaining a stable trust level could be to lower the trust level for the entire network, meaning: "because you can not share with some individuals, all sharing at this level halts". The interviewees were reluctant to use this solution. "Does trust grow fast enough for people to remember what the trust level used to be, I do not know. If you are in a situation where you have dropped the trust level, and if the time to build trust is longer than the turnover of people involved, you can get to a point where nobody remembers what level it could have been at. Then there might be little or no pressure to work to rebuild trust to this level." Another interviewee pointed out that even kicking a member out that has caused a fall in trust level might not help: "After a breach, the level of trust will start lower even if you have thrown someone out, the members have been reminded of trust issues: anyone should be prudent in choosing what to share with whom." Analogous to this is

[2]TLP: The Traffic Light Protocol was designed to enable clear classification of data in information sharing an communication. The codes are: RED - personal for named recipients only, AMBER - limited distribution, GREEN - community wide and WHITE - unlimited.

[3]NDA:(from Wikipedia) A Non-disclosure agreement is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by third parties.

airport security after a bomb threat. Even if the perpetrators are caught, the (in)security level is elevated.

In the Trusted Introducer network, one can revoke accreditation or certification of groups, as a means of rendering a stable trust level without lowering the general trust level in the group. This has never been used, but the review board has the mandate to do this.

There is some inherited trust in networks, but this phenomenon is difficult to grasp as it is counterintuitive; although all claim that trust is personal and human, there is some inherited team trust : “once you are a team, you are known and vetted and you have done good things, people know you, you’ve been to meetings and you have drunk beer, people trust you; you can exchange everybody on the team, remove the funding, change all the bosses but you will still be trusted for quite a long period of time.” Another of the interviewees had experienced similar phenomena, where she felt she gained trust quicker than normal in a network, due to some inherited trust. She postulated that “there is a conscious level of trust related to the position and an unconscious modifier of this, which is the person”.

The inherited trust described may support the idea of organizational trust as a more advanced form of trust, something that appears only with a strong basis of experience-based personal trust. However, the cases indicate that the organizational trust may be more at an unconscious level and that the personal trust as the conscious level, and not the other way around. This may be an area to look more closely at in the future.

The trust level in networks is organic. The more a network is based on a person-to-person trust, the less the trust level can be steered. One of the experts felt that some kind of middle way is appropriate, where the trust network accepts certain fluctuations in trust, but has processes for dealing with these to make the member feels more at ease.

4.4 Activity and network value

Incentives for joining trust networks is important, and an inevitable part of this, is the network activity level and the knowledge sharing done in the networks.

4.4.1 Incentives for trust network participation

The incentive for a membership is important to the networks ability to function properly and evolve. Parties that become members just to be present, or just to have their name on the membership list for the glory, is probably not contributing to the community as much as a member that is genuinely interested in making the network better by sharing information.

One of the specialists noted that some of the more active members of the network have been under DDOS attack some years back: “they share now, especially since they were attacked, they got a lot of help from a lot of people all over and that may be one of the reasons they are quite open, because they found that the sharing really works”. The positive results of the trust networks’ operations during attacks often make the benefits of the network memberships apparent to the funders, and with this justification, funding can become easier.

Several of the interviewees had a positive view on the coming certifications process in Trusted Introducer (TI). One felt that not only will this for some members be a chance to get a certificate of quality, but it could also benefit other teams. The certified teams can function as leading stars,

and their participation in TI can be an incentive for other teams to involve themselves, “to work with the role models”. Another of the specialists concurred, although she felt that the certification is not vital to this, that good leadership in the trust network can bring out benefits that will make the value of the network apparent.

4.4.2 Justification of cost

There are always costs involved in the memberships. Some organizations have yearly fees, some are government financed, and yet others are based on a shared cost model. In the latter case, each member covers some specific cost in the network, like hardware or meeting costs. One would think that inactive members of networks, would both feel left out and would gain nothing from the membership. One of the interviewees observed that they may have to explain the costs to management: “now if this costs a reasonable chunk of money, finance should ask what the local organization is getting out of it”.

A representative of a government sponsored network was of the opinion that the cost of joining a network should be as low as possible, and criticized some networks for existing in itself to earn money, questioning whether this might not tempt the “owners” to pretend mundane data is unique and important to assure the members of the value of the network. This coincides with disgruntlement in a membership funded network that claims to gather data to aid the sector within the country, where several members claim the network operators are just formatting useless data to seemingly justify their costs and even their existence. If this is in fact true, this is destructive, not only for the network, but for future attempts to form information sharing networks with these disgruntled parties.

4.4.3 Network activity

In evaluating the significance of network size, we briefly discussed the nature of the information shared, whether it was operational, meta-information or trends. One interviewee observed that “it is most often only at matter of sharing what is going to be open anyway” (early disclosure), and “if there was really sensitive information, a small network where all members can feel safe is important”.

Trusted Introducer is intended to be an operational network, alongside for instance EGC (European Governmental CERT). It is a network designed to be used for sharing of more sensitive information, but as two interviewees observed: “TI was a network to share sensitive information, but there is criticism now that the information was not remotely sensitive or valuable, even amongst the accredited teams”. Several of the interviewees claimed that even if data may sometimes be of organizational nature, activity in the network is extremely important; if there is no activity “you might as well pull the plug”.

One interviewee claimed that the information shared should not only be incident related, but rather event driven. Sharing the characteristics of normal traffic as well as incident-related traffic could enable the participants to baseline the activity, to assess the threat and discover relevant anomalies at an early stage. This is intuitively an ideal situation, and the idea of sharing the characteristics of normal traffic as well as incident-related traffic is supported by other teams and sharing initiatives. However, this activity would demand even more from the participants, hence increase the workload, and as one interviewee pointed out; “security groups seem to be

either too busy to gather and sanitize data for sharing, or maybe they fail to see sufficient value in this".

4.4.4 Competence

A trust network member's competence was noted as important by all parties, especially in a network where live, potentially sensitive data is to be shared. All parties need to be discreet and aware of the local disclosure terms (like TLP), and higher competence level increases trust, "you need to demonstrate that you being part of the network is useful to everybody else". This will often exclude politically or administratively appointed representatives. Another professional also pointed out that "a network must consist of people who are eager and knowledgeable, and will give something of themselves", which even makes demands to the participants' attitudes. The member (person or group) should have assets (information, contacts or competence) that is useful in the trust network, this is one of the overall main reasons to admit new members into trust networks - "it is all about the skills and the power of influence".

The control mechanism is partly inherent in the network, and as most networks have a vetting mechanism this weeds out the teams who do not have the constituency or competence they claim to have in the application process. And anyway, as one pointed out: "you do not have to sign that you have a certain competence, the network will find out pretty quickly what you are useful for".

They also state that being active and being at meetings is a huge advantage if you need to be vetted in somewhere, or you need help from the community in the event of an incident. The active will have more credibility and will find it easier to join or to form task forces to deal with specific problems and to make people share relevant data, even if all are part of the same trust network. "Activity means people or teams actually contribute and help, and do not just use or abuse the network for their own purposes".

A certification scheme gives no guarantee of the level of competence in the member's group, but it can however provide a certain "level of assurance of baseline competence, continuity and commitment" by the group, and gives the members a chance to benchmark themselves. The certification arrangement is however too young to be evaluated at this point in time.

4.4.5 Incidents and exercises

The general idea that a crisis brings people together also applies to trust networks and information sharing. This became very clear during the DDOS attacks on Estonia and Georgia in 2006-2008, and also evidently in the banking network during the battle of the Zeus trojan horse as observed by an interviewee: "Maybe the big incidents help? Where something is sufficiently obviously a threat, you forget the politics and just get on and fix it. That might actually be the way to re-build trust: sharing worked really well, how can we sustain that?"

Fortunately large incidents like these do not occur too often, and one way of building trust in a similar manner could be to organize exercises. The specialists were divided in the view on exercises as a means to increase trust. First of all the participants need to be dedicated: "somehow you have to persuade them the exercise is important enough, and you need to stop people from saying: this was only an exercise". Several of the interviewees also pointed out that one has to put a lot of work into making an exercise to make it as realistic as possible, but that exercises has great limitations and often do not work to any important purpose. One

specialist believed exercises are important, but she was careful to point out that what are the main purposes of an exercise: to reveal the chain of command, to clarify reporting structures, to make mandates clear and stated for later real life incidents. “For instance, the structure of organizations on a every day basis is seldom the structure you want to rely on in a crisis, you most often want a crisis management in a separate ad hoc organization. This can be revealed by exercises.” She has incorporated exercises as part of the security work in several groups, and feels that repeated exercises, especially in target problem areas, increases the possibility of effective crisis management in the event of a real incident. These claims are supported by several exercise reports[72, 39, 73].

Although the belief in exercises is limited among the specialists, none of them were directly negative, and the effect of an exercise in the evaluated trust networks considered in this thesis is unknown as it has not been tried.

4.5 Barriers to trust and information sharing

Some networks are specialized, and the description or mandate of the group clearly states who would be eligible for membership, but most networks have loose definitions of the member types. ISAC Europe, for instance, states that they “focus on critical infrastructure”. This gives no guidelines as to desired member organizations. In the protection of critical infrastructure you could include anything from a governmental CERT to the company that does physical maintenance on the infrastructure, you could include government agencies or the national cyber police. The main concerns when deciding on principles of the network membership has to be potential network size and potential mutual usefulness, but one also has to be aware of potential conflicts of interest or the chance that members may inhibit trust or information sharing, merely by their presence.

Several trust networks have included law enforcement. As one of the interviewees stated; “The main goal today is not like 10 years ago: just making an incident stop, make an attack stop and go away. It is now about prosecution, about catching who is behind it. So there is definitely a need for cooperation. In the end the CERT also wants the same thing: to catch the bad guys.”

Even in national networks, cooperating with law enforcement can be complicated. Several of the specialists were quite clear on this: “We should have had a better interface to the police, but bringing law enforcement into the inner circles can lead to people not sharing the information. An important reason people share is that they think they will be helped.” Several of the specialists state that their interface to the police should be better. Two of the specialists, however, described the domestic trust interface to the police as being thought through and well defined. One of them described: “The national police high tech crime unit came up with a very good information sharing agreement which they signed and committed to: whatever you provided they would treat as intelligence only, if they wanted to treat it as anything else they would get back to you, and you had the opportunity to say no. In the law enforcement system, there is stuff already that is not evidence and can not be used as evidence, hence it was not a big culture change for them, it was just a matter of writing it down. The agreement made people more willing to share because the boundaries of the information shared was clearer.”

The situation becomes more difficult when the trust network is international, one nation’s

law enforcement may have to report to external parties certain types of data, which was shared by a member from a different country, with a different judicial framework.

"There is a lot of nervousness when it comes to having police organizations inside the multi-national trust networks. I do not know if it is true, but there is a perception that in some countries the police can not just treat information as intelligence, that if they get something actionable they have to act on it." One relevant example of this are some countries' laws on freedom of expression, which may conflict with other countries' laws on slander or blasphemy. Larger, international networks should probably look at creating standard agreements for cooperation, with international law in mind.

Not only law enforcement gives raise to uneasiness in trust networks. Having any kind of regulatory parties or – authorities is controversial to most. Several of the professionals explicitly stated that having regulatory authorities involved would be leaving the fox to guard the geese, especially if an authority has the power to both certify and audit solutions.

Several of the experts believed that larger, international network should be public-private, that they should span as many sectors as possible, and that the networks who leave out or find private parties less significant, are mistaken. "Some networks leave out partners like MSSPs (Managed Security Service Provider) etc, which is a pity: one often uses third party companies for technical analysis after an incident."

4.5.1 Culture

A couple of the experts started out claiming that cultural difference should not be an issue but after a brief pause they thought it really might be an issue anyway, one said: "The trust level people experience with a culturally familiar team is bigger than with certain other teams. Their personal preferences might even be different from what they are forced to accept in some countries, those are just facts of life, but I am sure it reflects on the trust level."

The way the different teams deal with incidents differs greatly. Teams are governed by different bodies in different countries, but there seem to be some likeness in incident handling between the teams of similar culture.

A security team's influence or even power in their constituency varies. In some countries it is clear that the team does not have the necessary mandate to handle an incident properly – for instance by having no say over the countries' ISPs (Internet Service Providers). In other cases it may be difficult to even know how incidents are treated internally if they have a closed door policy, and treat all incidents information as "domestic sharable only".

In some regimes it might be difficult to know who is really talking, and who is governing the security work. If the regime is totalitarian, trusting that the team is free to follow NDAs imposed by a trust network is not self-evident. Even in countries where the regime is apparently well functioning, there might be controversies as to who should speak on behalf of the nation, hence also the controversy "what is really our opinion" and "is the mandate a real mandate". Politically unstable countries can also be a threat to trust as pointed out by two of the experts. One said: "In a non-stable country you may ask yourself; if you feed them steadily with incident information, what will this be used for in the likely event of a regime change? You can even put some in a difficult position because you have given them this information."

In one particular country mentioned, the government dictates who and how the CERT team should help, and possible conflicts of interests are apparently pushed aside because “the government says so”. One of the experts states that this would most likely not work in Europe, as people tend to be less willing to follow government leadership.

Several of the experts believed that for instance a pan-European and a pan-Asian network would function differently as the cultures are so different. They were all careful to make sure they support any group of people that form trust network to combat cyber crime. “Cooperating against cyber crime is always worth a try, even though I might not play with the whole hand dealt from the very beginning. You need to feel your way there.”

An Asian interviewee believed that there are cultural elements to consider. She sees the Asian communities as more hierarchical, and the members in trust networks as having more trust in the leaders or governing parties of the network than in the west. Asian leaders, she said, are not afraid to take full responsibility, as opposed to in the west where putting blame downwards in the hierarchy is more common. She finds that most Asian countries think less of individuals and more of “families” (literally and figuratively), and believes this can facilitate trust building.

She stressed that she is only familiar with parts of Asia and Europe, but she sees clear similarities in this area in the Asian countries. She feels the roles and mandates are clearer and there are more absolute rights and wrongs there, as opposed to here where tasks and roles are less specific, which lead to higher uncertainty.

Another type of coalition is the OIC-CERT, Organization of The Islamic Cooperation-CERT. Although some of the interviewees found it odd to have religion as a basis for information security collaboration, others pointed out that there may also be practical reasons for this, for instance that obtaining visa to go to other Islamic countries might be easier than obtaining one for the western countries. There is a process to enhance the collaboration between OIC-CERT and some other networks, but this is not entirely without controversy. Questions like “defaming the prophet – is that an incident” has been raised. One expert also stated that the basis for the western network is a Christian culture, hence the thought of a religious basis should not be all that strange to the community, while another of the interviewees did not see this as comparable.

The differences in culture are seldom discussed or addressed. In the large trust networks, all are treated equally. This may sound good, but one could imagine a situation where the individual cultural differences were honored. Increased openness could lead to better understanding. “It is important to understand each other to build trust, and with great differences in culture, this can be a challenge”, as one interviewee pointed out. “Nobody must feel that the others in the network do not respect and understand them. There are some countries that currently struggle to function as trust network members, even if they are big political powers. Some countries and continents are bigger CERT-wise, with longer traditions. All must however, understand that it may be necessary to talk differently to other cultures.“

Trust in a team is still based on the perception of the team’s willingness to work to solve security issues within the limits of their mandate, as several experts pointed out. However, the perception of this effort might be skewed by cultural misunderstandings, and if the intention is to improve the trust network across cultural borders, it might be wise to, as one of the experts advised “to take these differences seriously” .

4.5.2 Gender

Two of the interviewees identified gender as a potential barrier. One stated that in some cultures, inevitably, you will gain less respect as a female, and that these cultures would probably not have a female leader or negotiator. The other, stating she is not pleased with the situation, stated that in negotiating and initiating a collaboration with countries known to have such differences, it would probably be wise not to use female representatives, although she stressed that in regular operation in multi-national networks, such inclinations should not be honored.

4.6 Membership rules and guidelines

All trust networks have rules, written or unwritten. The rules vary from rules for becoming and maintaining a membership to code of conduct, and some specify frameworks for information sharing and also measures to be taken if the specified rules are broken.

An incentive for following network rules that was mentioned is the fear of repercussions, or even punishment. One of the interviewees claimed that “this may work for a while, but all dictatorships have turned out to be unstable and to fail at some point”. The Wikileaks affair was mentioned: “revealing data from the US armed forces showed that threats of imprisonment and even death penalty is not enough to keep people from sharing outside the intended group”.

4.6.1 Activity level

Some networks have either rules or recommendations for the activity level. All the specialists agreed that activity level is important for trust earned by the member. The one that participates silently is not trusted: “Being silent is not good. The one that participates silently is not trusted because he contributes nothing other than making the group bigger than it needs to be, and is therefore a risk.” Most trust networks do not have compulsory attendance at meetings, but they strongly encourage members to come to meetings from time to time. Trusted Introducer’s certification scheme actually demands the certified members attend 3 out of 10 meetings.

An issue that would need to be addressed if attendance frequency is to be weighted more is the economy of the member team, and the possibility to raise funding for travel etc. If the networks do not consider solutions to this, the network would in reality be limited to the wealthier countries. This is not a desired situation as many security incidents, especially fraud cases, has the perpetrators located in poorer countries. One definitely wants well connected teams in all countries. Funding from other governments is an option: “I would like to see certain parties provide funding for teams from poorer countries to go to a meeting once a year or so. Maybe even the EU could do this, they put a lot of money in under developed countries, why not in this area?” The network itself could of course raise money or dedicate an amount of the membership fee to sponsor teams, and one of the specialist suggested a simple solution for sponsoring: “We could invite them to host meetings”. If there is a cultural barrier that needs working on, this is probably a solution that should be looked closely at.

They all thoroughly agreed that compulsory meetings would not work, and that any forced measure would fail. However, some of the networks have other kinds of keep-alive measures. Trusted Introducer, for instance, requires each member to update team information every 4th month and some smaller networks have high activity requirements.

4.6.2 Information sharing

Another side of activity requirements is what you "bring to the table". Peter Allor in the FIRST Steering Committee said: "Information sharing is like pulling water from a well. To get the water to flow, you must first prime the pump. That means you put water into the well from your pump to prime it. And of course, you must feed the aquifer with water (information)." They all agreed that sharing increases trust: "The idea is based on the assumption that there is trust that information will be shared back, and the participants are encouraged to begin sharing as it increases the overall trust; you have to give some to get some."

To look at the problem from the opposite angle: Not only does lack of sharing not improve the network, but it damages trust in the team: "We have seen examples of respected organizations that have grown to be seen as an information sink. Information went in and nobody ever saw anything come out. And they have lost trust because of that. You have to bring something, but you do not necessarily need to be complete peers with the same amount of data to share".

One key factor in sharing is knowing with whom you are sharing your data. Most trust networks have mailing lists, but if the list subscription is not personal, it can create uneasiness in the sharing parties. This requires a maintenance at each member organization, a task that is trusted to each member. This is a natural inhibitor for the sharing of sensitive data on the lists, as you can not know exactly who will receive the data. Even tagging the data with the Traffic Light Protocol (TLP) is no good, if you do not know that the recipient will honor the code. Another, non-related problem with the TLP is as one interviewee pointed out, that "it is a gentleman's agreement with legal challenges, one nation's secret is another's forced shared information". However weak, most of the interviewees believe TLP is a good tool in information sharing, and several of the networks are at this time considering implementing it.

One of the interviewees participates in a network that has Non Disclosure Agreements (NDAs) with each of the participating parties. She was also very clear on the issue that the one whi is sharing information always knows exactly who will be the recipients of the data shared, after it has been sanitized. This is of course a sound solution, but with a considerable extra administrative burden. Several of the networks have clauses in the application concerning the treatment of data shared in the network environment, but in the case of bilateral sharing the parties normally agree on separate NDAs outside of the network.

4.6.3 Exchange of members

Most of the larger networks have team based membership, with one person in particular as the "main representative". It is left to the membership organization to ensure that the network knows the name of the representative. Most networks do not have any requirements for key signing from the old to the new representative or formal presentation of newcomers in a team. The interviewees did not see this as a necessity, since there is initial vetting and it is team based: "The teams are the members so this is the trust model". This would account for the aforementioned inherited trust, but it is not supporting the supposed need for personal trust. This may be because the personal trust is purely experience based anyway, hence takes time. An introduction only ensures the person is in fact in the same organization.

Several of them believed however, introductions would be a good idea even if an introduction

in itself does not create trust: “it would be nice if the previous representative recommended the new representative but I suspect on the human side it would not actually help much”. We know that some trust can be inherited, but if a lot of the crew is changed it might impact the trust level, hence formal introductions by existing crew members would probably be a good idea.

4.6.4 Breach of trust

Most trust networks have procedures for handling a breach of trust, and all the interviewees believed there should be investigations and possible repercussions following a breach. Several stressed that the culprit should be given the benefit of the doubt as breaches are most often due to eagerness to share or mistakes made by an individual, hence the team should be given the chance to investigate internally: “That the team has to tidy up internally first is due diligence, if they do not do this, the confidence is broken.” One of the interviewees was a particular advocate for a more open fault culture: “It is important to make sure the problem is dealt with to restore trust. A good thing is to have an open fault culture. This strategy has great success with the airlines, people are encouraged to report faults, and they actually do”. Intuitively this is true; someone who openly admits a fault is more likely to be trusted than one that is discovered by other parties. This is something politicians have learned, as they always try to admit to faults if they know they probably will be caught. As with any information sharing, the reporting of faults will not catch on unless some of the “leading stars” in the community initiate such reporting.

All agreed that there must be repercussions if the breach is more than a small mistake. “There has to be repercussions, an investigation into what happened that lead to the breach, ultimately one may have to suspend a membership in a trust network. The owner of the information would ultimately be the one that decides the severity of the breach.” Even in the presence of a formal NDA or a TLP coding, the owner of the data is the only one who can decide on the value of the data, hence the severity of the breach. However, it is important to the community to see reactions, one of the specialist muses: “it makes no sense to set up the TLP if it is not enforced. This is a thing that is often overseen.” In some of the smaller, very strongly vetted networks, a breach can lead to not only exclusion, but also the exclusion of the recommender.

One interviewee believed some sector networks might be slightly more resilient to breaches than the larger cross discipline networks, “They would have the formal framework, I suspect they would recover more quickly and more uniformly.” In a sector based network, the members will also be more likely to have a better understanding of the value of the data shared, and also an understanding of the consequences of a possible breach.

5 Discussion

Security professionals seek to find trust-enhancing measures in order to create networks that can be a fertile ground for information sharing. The goal is to make the knowledge of one network member part of other members' complementary knowledge, which in turn will lead to cost reductions and better security for the individual member and for the society as a whole. The networks seeks to enable mutual help in cyber attacks or similar incidents, and to make the attack patterns more transparent by sharing information. Such networks have already proved useful in attacks like the ones on the Estonian government in 2006 and the Georgian in 2008.

However, sharing this type of information in a network, might leave you vulnerable. This is similar to basic game theory, or the prisoners' dilemma. If no one shares, no one benefits, and if both share both benefit. If only one party shares, it might be an advantage to be the non-sharing party.

In this chapter we discuss our findings from all sources, in relation to the hypotheses (see page 4 - 5).

5.1 Network size - Hypothesis 1

Quite a few trust networks have emerged during the last 10 years, and some of these have grown large. The question that arises is whether there should be a limit to the number of trust network members. This is however in our opinion purely an academic question as it would not be reasonable to refuse membership for an organization, purely on the grounds that it is member number max+1. Literary sources on trust, as well as discussions around the matter reveal that trust is a complex matter, not only is trust multi-layered, but it is highly context dependent.

As the number of participants in a group increases, it becomes increasingly difficult to know everybody personally, and as all interviewees agree; trust is a personal thing. However, looking more closely at the trust level needed for information exchange, we find that the size of the trust network is also dependent of the type of information shared (Jianghe Niu[30]). Intuitively this is clear, but this does not mean that information shared in a larger, lower trust level, network need to be irrelevant or unimportant.

First of all, the network can be, as one of the interviewees claimed FIRST to be, a meta-network. This would function as a trust forger, and an enabler of trust, it would introduce parties that could later participate together in tighter knit organizations or in incident handling. Brewer and Kramer[51] claim larger networks lead to de-individualization and a larger chance of free riders. This may be so, but if the expectations of the participants are adjusted to meet the reality, their idea of network trust quality is also adjusted (by definition). If the participants all agree on the goals and visions, hopefully the level of information sensitivity and network dynamics will follow.

The important thing when creating or revising a network would be to prepare for a large size network, to agree on the purpose of the network and to take appropriate measures to support the

growth. This could be in analyzing the dynamics, in creating supporting trust structures within or surrounding the network, or in setting up mechanisms and activities to enhance trust. The need for vetting and face-to-face meetings in the “mainframe” network is still important. First of all, there has to be a certain trust level to make participants want to contribute in any way, and second, in a crisis where immediate collaboration is required, the members are likely to take a slightly higher risk, letting transitive trust be sufficient for even deep level information sharing; you need to trust someone purely on recommendation, and this is easier to accomplish if the parties have already met, even just briefly.

Both the interviewees and studies superficially back up Hypothesis 1 (p. 4), but the statement turns out to be too simple. Trust is always in a context, so “real trust” is contextually conditioned. One could say that there is a contextual size limit to groups to share information at a certain sensitivity level, but this in itself is not a very useful finding.

5.2 Network types - Hypothesis 2 and Hypothesis 3

In the wake of a discussion on network size, the natural problem that arises is network structure, or network type. An obvious way to limit the number of members is to organize the network hierarchically. One might think this is a better structure for enforcing policies and rules as well, but several interviewees state that historically this has not shown to be a good trust network structure. This might be mostly true in individualistic cultures, but nevertheless relevant.

The bilateral trust between the delegate and the constituency is especially important in hierarchical networks. The constituents must not only trust the delegates intentions but also trust their abilities and competence. The delegate may also meet situations where the views of the trust network is opposing to the general view of the constituency. This can be a challenge to both trust relationships.

Another challenge to hierarchical networks is the individual contributor’s need to have strict control of her own data, and being able to herself take control of the release of information. It is also important for contributors to be seen, and to be given credit for contributions.

One interviewee mentioned that sometimes one should recognize that oneself is maybe not the best one to contribute in all situations. While this is true, this can quite easily be contrary to human instinct. Most people have a tendency to value their own contributions and trustworthiness higher than others, as pointed out by Jianghe Niu[30] and Elahee et al.[31]. This complicates matters and makes it harder for people to accept participation by representation.

In a hierarchical network there would also be a substantial delay in information exchange between “leaf nodes”, which in this case would amount to the actual incident handlers. The information would have to go up in one hierarchy, and down the other. This could be a disadvantage when working as a large virtual team in large incident handling. Most of the interviewees were sceptical to hierarchical trust networks, which supports Hypothesis 3 (p. 4), and their argumentation is consistent with a substantial amount of literature (Wall[60], McDermott and O’Dell[56]).

A hierarchical structure as only a point of contact (POC), for instance per country or per sector, is an entirely different matter and does not require such a complex internal trust structure. Complications can arise in these situations because an incident does not limit itself to for example

Figure 11: Countries spanned by a multi-national network vs. the borders of “Europe”

“Europe” or one network provider in particular. Making sure the information trickles down to the appropriate parties may not be straight-forward, even if it may seem like an appealing idea to for example large technology companies based outside of “Europe”, see Figure 11.

In all cases, one would have to make sure that the network had no single point of failure, if a representative or the top leader is compromised in some way, there must be a contingency plan. This would, of course, be important to all network structures, but intuitively a hierarchical network is more vulnerable.

Another way of dealing with large networks is to tone down the sensitivity level of data shared in the network, although this would surely happen dynamically anyway. One could try moving the more detailed work and data sharing into smaller groups, special interest groups (SIGs) or Communities of Practice (CoPs) . The network can spawn smaller networks for participants that have special competence in the relevant area. The SIGs/CoPs are celebrated by both the interviewees and many other experts, for example Wenger and Snyder[54], Loss et al.[29] and Msanjila and Afsarmanesh[19].

These smaller groups tend to inspire professionals. They have more mutual commitment and less conflicts. Another advantage of these network is that the vocabulary will be more uniform, creating less misunderstandings. All in the group will be at approximately the same level of competence in the relevant area, hence be able to create a shared identity by merging knowledge into a common pool.

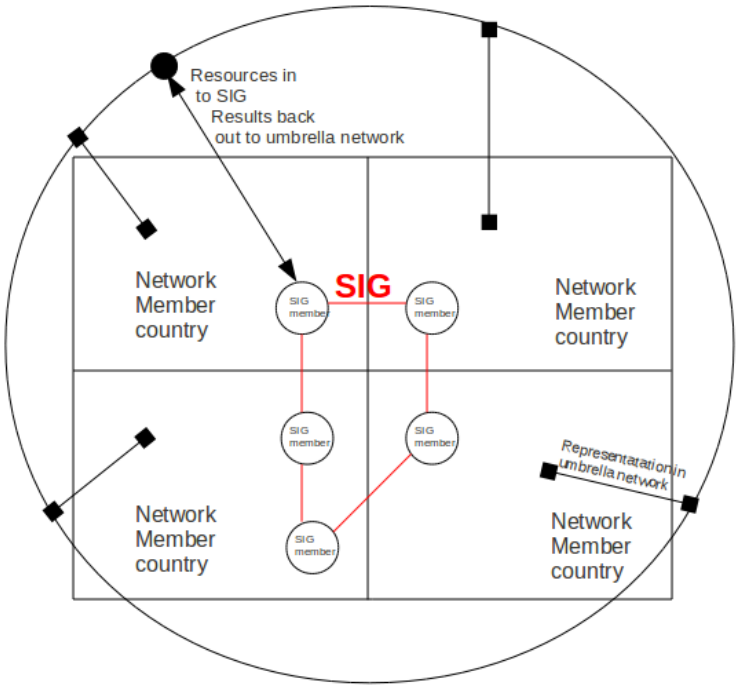

Figure 12: International SIG with members from different countries that are represented in the international "umbrella" network. The "umbrella" network supports the SIG, and gets results back out.

An important factor is that the groups need clear goals and milestones, and may need support in the form of technical frameworks, secretarial services etc, which should be provided by the "mother network", especially if one considers the SIGs to produce something of value to the network. The structure of such small groups do not have to be dictated, the work form and trust bonds create the network structure, one can formalize structure later.

There is need for transparency between the large and the smaller networks, enough to provide assurance to the members of the mother network that the work in the smaller groups is worth supporting and that it is serving its purpose. This should however not turn into strict control mechanisms that becomes a straitjacket of excessive reporting, limiting network creativity, see Figure 12. Even though the network depicted here might seem similar in structure with hierarchical networks, there is a difference; even if a SIG/CoP may have someone responsible for keeping in touch with the mother network it is not a "chain of command", the structure is relatively flat.

Both the interviewees, other security experts and literature support Hypothesis 2 (p. 4), that restructuring in smaller networks, possibly surrounding or supporting a larger network is a noteworthy solution to challenges of network size.

There are a number of ways a network may be organized, and not only does trust form the network, but it is formed by certain strategic decisions and bonds, by cultural alliances and other existing structures. The OIC-CERT is an example of a trust network that is built on existing structures, namely the governmental structure "Organization of Islamic Cooperation", another

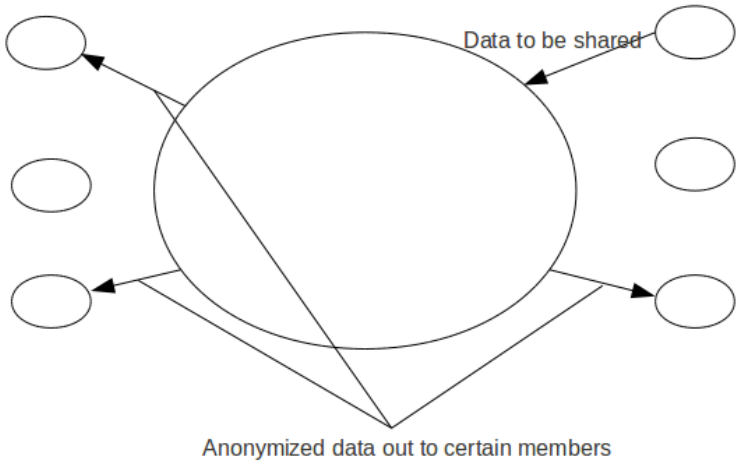

Figure 13: The Melani structure; the hub receives all the data, sanitizes it, and shares it back to the relevant members.

structure is the EGC, the European Governmental CERT coalition, which is an informal group with self-explanatory target audience. We have not had the opportunity to evaluate the efficiency of the first network, but the latter is supposedly a productive and sound trust network, and one could use existing trust structures like these as corner stones when building other larger trust networks. The EGC is a form of sector network, and there are several other sector networks, but none that span worldwide. In sector networks, you potentially get an insight into what that particular type of industry/organizations see as their main threats and receive information about current attacks. Depending on the sector, it can be difficult for a sector to have enough competence in all cyber security areas, so membership in several networks is probably recommended. Yet another example structure is the MELANI network in Switzerland. It is designed to enable information sharing in critical infrastructure domestically, they function as a help desk, organize workshops and are an information sharing hub. The members are from several sectors, with a majority from the financial sector. The reviews are positive and the hub in this network is seen as neutral and reliable by the members, as reported in the 2010 evaluation[84]. These are interesting results for domestic affairs, but not a solution realistic to implement internationally due to the required trust the member will have to place in the hub see Figure 13.

5.3 Network dynamics and governance - Hypothesis 4 and Hypothesis 5

The trust level in a group is never static, the changing of members, the sharing of data, breaches of trust; all incidents small or large, affect the trust level in the group, see Figure 14. Both the interviewees and literature back up the claim that building trust takes time, and that trust can not be forced or commanded. Cooperation can be forced, but cooperation is not the same as trust. One may even say that trust is the replacement of control and command. Deterrence based trust can not be considered real trust as one will never know whether someone has good intentions

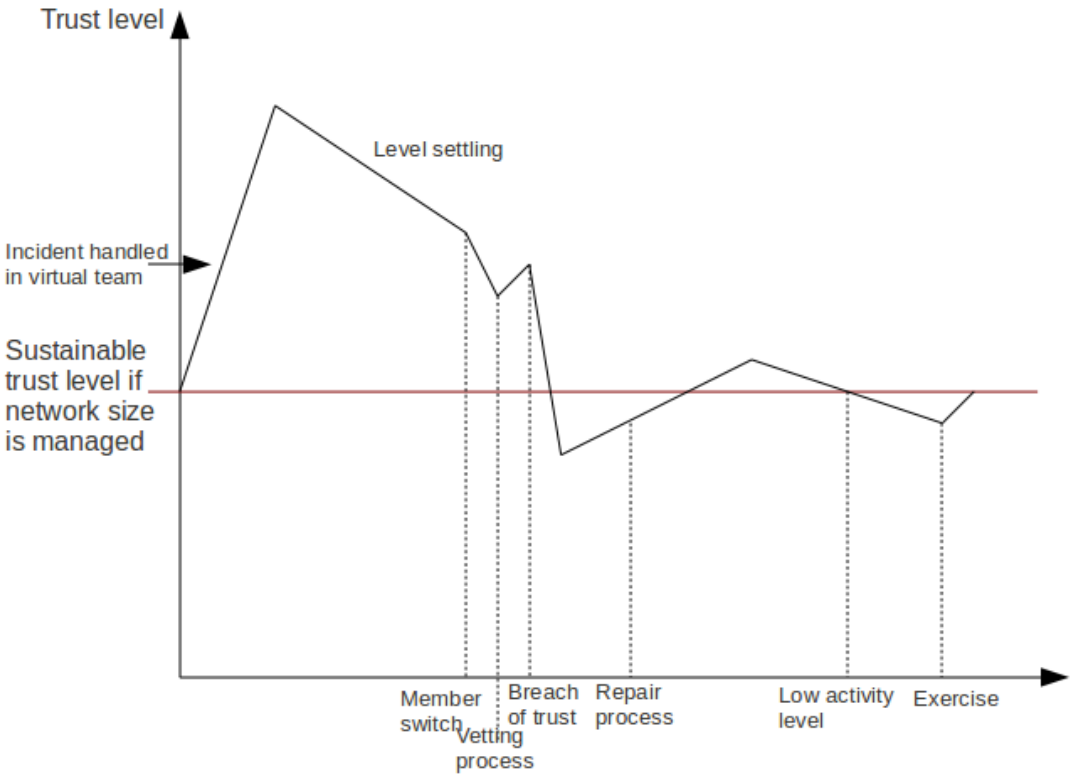

Figure 14: The network trust level is all the joint trust of all members. When representatives are changed, when there is a breach of confidence, or there has been a successful cooperation handling an incident, the trust level changes. A higher trust level is desired, but may not be the most stable and predictable situation.

or just wants to avoid punitive actions. It is easier to tear down than to build trust and the goal in governing a group would be to keep the trust level as steady as possible, and to create predictability.

It is appropriate to emphasize that thoroughly educating network members in the governing guidelines, rules and regulations is imperative to avoid breaches caused by mistakes. Members can not avoid pitfalls if it is not clear what to avoid.

Introducing new members in a group will lower the trust level. All trust networks have some kind of vetting, and the smaller the networks are, the more the vetting is trusted, as the links are stronger and the network more robust. To minimize the drop in trust level when new individuals are introduced to the network, one could increase the perceived value of the newcomers, Shaw[10]. Honesty and transparency in the vetting process, as well as honesty from new members about competence as well as integrity is imperative. Also; an increased number of trustees/higher number of vetting teams lessens the perceived risk in trusting the newcomer, a “safety in numbers”. The process before and right after the admittance of a new member should make the newcomer’s intentions, capabilities and trusted connections clear to the rest of the

network.

If someone is representing a group membership, replacements are inevitable. This will drop the trust level in a network, but some measures can be taken to minimize this drop, for instance having an overlap and introducing the replacement, preferably face-to-face. All agree that this is a good idea to initiate the trust building process, but in most networks it is not being practiced. One can also operate with a deputy representative, in which case the network would already be familiar with the new representative, and the trust would already be based on some experience.

In the event of a breach of confidence, both interviewees and literature indicate that an apologetic approach/admission is the best way to repair trust, as far as it can be repaired. For the "accused" member this is only partly true, it depends on the evidence (Kim et al.[65]). As mentioned above, if the accusation is backed by weak or circumstantial evidence only, chances are the other members will not let one potential false accusation tear down existing trust bonds (Rousseau et al.[18]). On the other hand, denial of guilt when there is sufficient evidence of the opposite, adds insult to injury. Another factor is that measures would differ in a case where the reason for the breach was due to lack of competence from where it was due to lack of integrity[65]. A glitch in competence can happen to anyone, a glitch in motives or intent can not. Again, the hypothesis, Hypothesis 4 (p. 4), was too vague. If the breach of confidence is based on integrity, restoring trust to the same level as before the breach is probably impossible, as supported by interviewees and the literature. But if the evidence is weak or the breach is based on lack of competence, the level might be possible to restore.

Leadership, and coaching of the parties involved in the breach is extremely important, and a sufficiently transparent process to avoid speculations in the network should be sought. At the end of the day the fate of the changes in trust level is in the hands of the "victim". If this member leaves the network because of distrust, it could lead to dissolution of the whole network. A trust network where there is considerable distrust is counterproductive. Both the literature and the interviewees support Hypothesis 5 (p. 4), about the importance of a clear leadership role. Although it is in the hypothesis formulated as "the leader", it would probably be more accurate with "the governing function".

The leadership role should be defined to suit each network type, some networks may benefit from defining different leading roles for different tasks. Existing networks have different policies on how the leading persons/group/committees are chosen, and whether the leadership is rotating, and even rotating from continent to continent like the United Nations prefer to do it. The important thing is that the members not only accept, but also support the method. Studies show that multi-cultural teams may have advantages in keeping the trust level more stable (Elahee et al.[31]), though this might also be partly due to a lower level altogether, or even due to something like a political correctness.

An entirely different side of trust network dynamics is the forming of crisis teams, or ad hoc incident response teams. We do not discuss this further in this thesis, but beyond any doubt, an existing trust network enables quicker and more secure forming of incident handling groups. Even if all the parties involved are not members, the networks forms a basis for communication, a structure that does not have to be built from the bottom up at a moment when every second counts.

5.4 Activity and network value

5.4.1 Incentives for trust network participation - Hypothesis 6

There must be a perceived value of the network to make potential members join, and for them to make an effort and participate actively. Even if the representative may see a value, often the costs, whether time or money, have to be justified to the company or organization. The process of weighing potential negative consequences vs. positive gain also includes considering the potential consequences to the reputation in sharing negative incident information, or considering whether information potentially can give strategic advantages to competing companies in the same trust network. The potential consequence of the latter is complicated and have, as far as we know, no known prevention mechanisms, see section on barrier of trust on page 59.

One of the main incentives for companies to be part of a trust network or information sharing initiative, is of course the expectation that the data sharing will contain useful information. The smaller companies or organizations would potentially benefit more from a cooperation as they have less data to analyze and learn from, and naturally less data to share. Lack of data can be compensated for in other ways, for instance by sharing their expertise. If a company is low on expertise as well as data, it will probably not have the ability to efficiently utilize the information received either. Hypothesis 6 (p. 5) and its corollary, is well supported by all parties. Receiving information, either for cost benefits or as an early warning is the main incentive for joining the networks, and without sharing the network will wither and die.

Cost savings is an incentive of high importance. In a well functioning network, this is quite visible. The savings can stem from shared development of tools, from increased detection of malicious activity, hence incident prevention, or from quicker incident analysis, hence shortening the recovery time. The network members who have been in a situation where these network functions have been needed, i.e. have been under some kind of attack that was at least partly resolved by the network, tend to be more trusting and active in the network afterwards.

Network membership and activity can also function as an improver of reputation, signalling not only that the member has competence and is considered important enough for membership, but also as a sign of power; there are resources, control and self-confidence enough to share data. Incidentally, this is something every member should keep in mind, as the influence on reputation is bilateral. The individual member can affect the network's reputation as well. However, the reputational advantages, as well as advantages in gaining influence and the benefits of external expert analysis are not rated as important in the ENISA study [67]. This may be true for some, but we can also keep in mind that it might be slightly degrading to admit to "needing help" with either improvement of reputation, influence or competence. Also; the incentives of the in-depth security expert may not be the same as the incentive of the management, even if they pull in the same direction. A interesting fact pointed out by one interviewee is that the "bad guys" have extensive information sharing and large networks of accomplices. This alone should be an incentive to find trusted partners to share information with.

A possible solutions that has been voiced is for governments to create incentives in the form of tax- or other benefits for those who join. This would probably be no better than trying to command it, there has to be a will to share and a potential for trust, the incentive should not be purely monetary.

Not all networks that are formed to protect critical infrastructure have focus on establishing trust relations at all. We believe this is a mistake as trust itself is an advantage in governing the network, and you avoid situations where members try to withhold information which would put them in an unfavorable light.

5.4.2 Network activity - Hypothesis 6

Activity in a trust network is important. For one thing, the network needs to know that the members are still functioning in the same manner as when they became a member; to know that they have not exchanged trusted members without notifying the network, that they still have the same contact information etc. If a member is active, these kinds of updates come naturally, as the member is reminded to check team/member information. Sharing increases trust in the network, increases mutual respect, feeling of commitment and reduces alienation (Constant et al.[70]), and importantly: sharing information keeps up reassurances about the individual member's benevolence, which is imperative in the calculation of risk before making a sharing decision.

If nothing is shared, the network will die, and rightly so. The sensitivity level of data shared must be adjusted to the network, one shares at the level that was intended in this particular network. Most data shared will be sanitized, either by the sharing party or as in the MELANI network, by the central trusted point of contact.

There is a fine line between sharing too much and too little. If the information is shared just to look active and in fact is worthless (old, not interesting etc), the other members will soon realize this and it will be counterproductive. Mandy Messenger[38] found that people share because they expect to receive data of "equal value ". This is supported by the ENISA survey [67] that states that data should be timely and specific, and interviewees from this survey actually saw poor quality information as one of the greater barriers to information sharing (see page 59). This is probably because the sharing is perceived as either done by someone who lacks experience to see what should be shared, or by someone who wishes to receive information without disclosing anything.

This should however not lead to too much hesitation before sharing; if the data is believed to be of interest to someone, this should suffice. Most trust network members enjoy helping, and helping someone gives the helper in turn the chance to show their usefulness. But if a member shares too much sensitive information, the network can judge this member as less competent, unable to evaluate how to handle sensitive information properly, or judge the member to have insufficient control. This, in turn, can result in the other members' reluctance to sharing with this seemingly promiscuous party. "How can one trust this member with information when they clearly can not treat their own information properly." It is fully possible to share data that are specific enough to have value, but sanitized enough to keep it at a sensible level. There are cultural variations in willingness to share certain types of information in different trust networks (Jianghe Niu[30]), but this is beyond the scope of this thesis.

If a network member is to share with members that have not yet shared anything, they can insist on mutual sharing, halting the process until the information flows bilaterally, or conversely, they can be "the bigger person". They can become a "leading star", which will actually also give the member a good reputation, rising them above in the social context (Constant et al. [70]).

Trusted Introducer has initiated a certification process which has a value in its own. It gives the teams that go through this process something to show for it. The teams that have been certified so far are clearly teams that normally would be “leading stars” or potential role models. Teams like these, and a regime like this certification could be something that sparks activity in a network. The increase in activity could appear both because teams actively tries to get the information flow starting, creating an environment where information sharing is perceived as the normal situation, or it can be because the other teams also want to go a little further, to accomplish accreditation too. The accreditation scheme is quite new so it is too little early to draw any conclusions.

The process of judging other members’ trustworthiness is a combination of evaluating the expected behavior and activity from these members. The process starts with assurance and vetting, and to reach a critical point where people feel comfortable sharing information may take some time, but can certainly be reached faster if the new member shares and is otherwise active. If people can not see what a member is doing, how can they know what the member represents (Williams,[64])?

5.4.3 Incidents and exercises - Hypothesis 7

The only time you see whether a network functions as well as intended for information sharing is when you work on real incidents, or maybe exercises.

Real incident handling is the best way to test the network functionality, confirmed both by the interviewees, the ENISA study[67] and experiences with the situation following the attacks on Estonia and Georgia. There was more information flow in the networks during these events, and there was a general community feeling, probably because the members mostly put possible reservations aside and worked together at the specific problem. In these situations there is seldom time to build trust in a regular fashion, the parties involved just have to assume there is trust and work as if it is so. To be able to sustain these dynamics and this high level of trust is unrealistic, but normally the trust level would settle higher, and the information flow would be larger for a while. If not worked on further however, the effect of the incident will disappear over time.

Even if joint incident handling may be the optimal method, waiting for real incidents is suboptimal, one should ideally be trained before incidents hit. Also, incidents include a random part of the network and statistically the attack rate is not uniform, neither is the knowledge distribution in the network. An exercise can be tailored to show a variety of scenarios and knowledge centers, permitting everyone to contribute.

The efficiency of exercises is debatable. It takes much work and well thought through scenarios to make an exercise realistic, and one of the most important factors is making the participants see the value of the exercise. This is the responsibility of all representatives in the network, and if whole member teams are to be involved, reaching a common understanding of the importance of the exercise is the responsibility of the team leader. It is all a waste of time if some parties go through the exercise with an attitude of nonchalance and superiority. Not only will they not follow the procedures they would follow in a real incident, which means the other members do not learn anything about their capabilities and procedures, but this kind of attitude spreads quickly, “it is only an exercise”. When people are asked about the efficacy of an exercise,

they build not only on their experience, but on the judgment from trusted colleagues, and if the samples are few, the result can be somewhat random. If the ones asked are also the ones organizing the exercise, it would be difficult not to be biased, and if the participants are being judged on the exercise it may be difficult not to become defensive.

There is general agreement that exercises gives the participants a clearer view of the abilities, goodwill and methods of other members, and as such is at least good for team building. Exercises are also suitable for testing virtual crisis team set-up. This should be tested under controlled circumstances, so everything is prepared for the real incidents. Exercise may expose internal organizations methods in companies, leaving some potential participants worried that exercises disclose potential harmful information about them.

Although some interviewees were sceptical, this was particularly because the goal of the exercise was not specified, and also it was assumed that people may not take it seriously. However, looking to the reports from different exercises and from ENISA, the exercise work looks promising, and it might just be a question of doing very thorough preparations. We would say that Hypothesis 7 (p. 5), is neither supported nor falsified, exercises may be a good tool to create some types of network activity.

Low trust/high risk networks may be the networks that benefit the most from exercises. Examples are military intelligence or other intelligence networks. They are governed by political units, and one of the traits is that they do not trust other countries' intelligence. These networks do not even potentially have the same dynamic flow of information other multi-national networks can have. Incidents where the cooperation in these networks are acutely necessary are rare, hence exercises are necessary. These networks are spawned from environments that are used to exercises, hence there is precedence for taking them seriously, increasing the likeliness of success.

5.5 Barriers to trust and information sharing - Hypothesis 8

There are a number of potential barriers to trust and information sharing, and we choose to focus on a few that are identified by several of the security professionals.

Competition between members in a trust network can be a barrier. Whether it is market driven competition, competition between publicly funded authorities or just plain human nature competitiveness, it can still lead to the withholding of information to give other members a disadvantage, and preventing network transparency all together. This is difficult to prevent. Sector based networks may be a good way to see the particular threats to a certain industry, but it will inevitably also bring cooperative conundrums on account competitive issues between the members.

The national laws of different countries, and the lack of international legislation is a barrier. For one thing, the ownership right to data differs and the right for the national authorities to access/read data that flows within the borders differ. Another matter is whether the individual member has an obligation to report potential "illegal data" to the national authorities, especially taking into account that the data is not necessarily illegal in the country where the data originated. This would especially be an issue for law enforcement or legislative institutions. Hypothesis 8 (p. 5), is thus not supported. Although scepticism against involving regulatory authorities and

law enforcement, the general opinion seems to be that this can be regulated and agreements drawn up, as pointed out by some interviewees.

Both the aforementioned competitive and legislative barriers can and should be fairly strictly regulated. These are predictable areas, and areas that are normally governed in other settings anyway, so predicting most potential conflicts of interest should be feasible. However, there still has to exist trust that the member will actually honor these agreements and rules, that they do not share the information wider than agreed upon. If a country should for instance outlaw encryption, this would constitute an impenetrable barrier to information sharing.

Fear of loss of reputation can be a barrier in several settings; a member might be afraid to share data from break-ins since that might make the organization seem insecure. Or the member may be afraid the information they share is uninteresting or wrongly interpreted, leaving the organization looking ignorant. These issues is a matter of trust network culture, and as part of network governance these things must be addressed. There will always be someone more knowledgeable so there should be no shame – one should embrace the advantages of extra expertise, and even if the data may be trivial to some, it should not constitute a problem if the intentions behind sharing are good. As to shame over incidents; there will almost always be organizations that have "worse" incidents. People tend to talk more favorably about each other than actual experience would indicate, and people know that the actual value of the information can only truly be assessed locally, so sharing seldom leads to loss of reputation, with an exception for the sharing of somebody else's information, or information as an inappropriately high sensitivity level.

Many of the elements that are perceived as barriers of information sharing is actually lack of trust. For instance would "fear of leaks'", as mentioned in the ENISA report[67], not even be present if the members trusted each other. Other perceived barriers like "group size" or "type of participants" is a question of management: how the network is defined, regulated and governed.

5.5.1 Culture - Hypothesis 9

Trust is influenced by the trustor's perceived risk in exposing vulnerabilities to the trustee. This means that the trustor must believe that the trustee is benevolent and predict how she will act, which is difficult to judge if you do not understand the relevant values and norms.

The key trust element in a multi-national network is to acknowledge and respect cultural differences, many of these are to the network's advantage, not disadvantage. Studies show that multi-cultural teams can outperform homogeneous teams (Gelfand et al.[59]). Differences that will pose a problem for the functioning of the network should be met, not necessarily avoided. Something that happens due to a misunderstood political correctness is that everybody is treated equally. This may leave many in a situation where they are not treated as they would prefer. However, there is no need to focus particularly on the differences itself, it is much more important to focus on the similarities between the members, such as security challenges and goals. This idea is supported by most of the interviewees, those who had an opinion on the matter, and widely so in literature and articles written from different culture's viewpoint. We consider we have support for Hypothesis 9 (p. 5), that political correctness in cultural diverse networks can possibly be damaging to trust.

When creating or revising rules and best practices, bringing in multiple cultures enables the group to easier see potential pitfalls. One must for instance decide whether the network in question is better off with a rotating (possibly also culturally) leadership, or a "familiar and stable" leadership. It might also be a good idea to revise the governance and trust level dynamics after a while. The younger a network is, the more frequent one could do revisions to be sure to settle on an optimal solution. The definition of culture is vague, but in a setting like this, one has to have rough division, even if someone does not feel represented, this can still work if the process is transparent. There is no need to understand each little element of all cultures, just the ones relevant for the network communication.

Another important element is clarity in messages, rules and structure. In some cultures roles are traditionally well defined, while in others they are "made up as they go". If the members per default for instance just expect the "leader role" to contain a set of certain implied qualities and responsibilities, some are bound to be either disappointed of confused. One of the interviewees believed some might even deem the leader incompetent for not fulfilling what they believe are the leader's duties.

Some cultures are individualistic and some are more collectivistic, where the collectivistic are more group aware (small or national) with a high degree of mutual assurance and perceived stability (Kramer[27]). This naturally affects trust. Collectivistic cultures are more sceptical to strangers from a foreign culture, than those from individualistic cultures are. On the other hand they are more trusting to strangers within their own culture than the ones from individualistic countries are (Yuki et al.[28]). If possible the best approach would be to accommodate the culture that would most easily find a situation offensive. Most cultures are more sceptical to "outsiders", some more than others, so if possible, when dealing with new network members or negotiating with external parties, having someone from a similar culture doing the negotiating or membership discussions could smoothen the process.

A variety of elements may be valued as important in a negotiator or communicator, like age, education, work position or gender. All these may be impossible to accommodate, and whether one should accommodate them at all is debatable. One might want to accommodate a culture as much as possible when negotiating or discussing on their turf. However, if the network is multi-national and multi-cultural, one must consider the work within the network to be as neutral as possible. That said, it might be wise not create rules for what not to wear, whether this is pertaining clothes or symbols of cultural (including religious) belonging.

Over-generalization over cultural or national issues is unfortunate, both because you can not trust superficial cultural indicators (Jianghe Niu[30]), and it can be perceived as offensive and prejudicial, which they in fact can be argued to be. One of the interviewees sees this as damaging to trust, for example the statement "country X is attacking company Y", is far more offensive than saying that "a group from country X" is attacking, and she feels that this kind of generalization brings everybody from the "accused country" on the defensive. These details are important to make multi-national communication more constructive.

If it really is so that there for some reason is a distrust in an entire country, this has to be addressed. This would probably be due to some political situation. For example could a sudden change in government lead to doubts whether the trust network member was compromised.

This should be sought cleared up as quickly as possible. There might be a need for a (possible temporary) suspension of the member, or conversely there may be a need for the network to reach out an help the fellow member.

The language barrier is a big challenge, not only inter-continent, but also intra-continent. It is important that information is kept in a fairly easily accessible language, e.g. having active form of a sentence instead of passive and using shorter sentences and simpler language (Connaster[85]). Simpler language does not mean less technical, it still has to be at the appropriate technical level for the group in question.

All cultures have a fear of loss of reputation, but some more than others. One is always more sceptical to people that are different than oneself, especially in these times where nationalism is on the rise in many countries (Schmidt and Rosecrance[86, 87]). These are barriers, but they can be mitigated by promoting and sustaining a sharing culture. All experience show that trust and information sharing increases with activity level. Some high avoidance cultures feel more comfortable with rules and regulations and have stronger faith in institutions (Doney et al.[12]). Both to accommodate this, and to be a foundation for trusted information sharing there should be a sound technical framework, transparent processes and clear and consistent rules of engagement. The framework chosen should be appropriate for the network type in complexity and form, the other elements are summed up on page 64 in a set of recommendations.

6 Conclusion

This study is based on the interviews of nine security experts from seven different countries. In addition to this, our personal trust network experience and relevant literature in the area formed a basis for the work on the hypotheses chosen. Our conclusions and findings include a set of recommendations for trust network building and maintenance. We only include recommendations that are not already thoroughly covered in the literature.

6.1 Summary

All agree that sharing security information, and in particular security incident information, is essential to increase preparedness and to battle cyber crime. The decision of with whom to share, however, is complex. The key element is trust, and trust can not be forced or commanded.

The decision does not become less complex when we want to share with many in a trust network. When the network grows larger, there will neither be sufficient direct, experience-based trust nor short-chained transitive trust to trigger positive sharing decisions. Studies and interviewees favor smaller working groups surrounding a larger network, keeping the trust level high in the smaller groups. We find however that the trust level could and should be kept at a high level in all networks, but the type of trust and hence the information shared will be context dependent.

Trust level in a group changes for a variety of reasons, and some fluctuations must be acceptable, especially in a "backbone" network. If these fluctuations are acknowledged, rather than ignored, the trust level can to some extent be rendered predictable, which is a key element in trust decision making. It is important to design guidelines for a network, and prepare for the inevitable trust fluctuations caused by new members, breaches of confidence etc.

A vital component in a network is activity and steps should be taken to govern the activity level to some extent, in order to avoid a dwindling of the trust level.The members are the only ones who can create activity, but a framework of support with meetings and exercises could be created to ensure a sustained activity level.

If there is a desire to keep networks multi-national, cultural diversities should be addressed. Political correctness can be a threat to trust in this context, in the sense that relevant cultural differences are ignored. Involving members from multiple cultures to form the network, in for instance writing or revising guidelines, would ensure a certain level of diversity, and striving to focus on common visions and individual assets is productive for network unity, and hence trust.

Even if trust is the vital component in these networks, the support of a framework for communication and information sharing is important, this and unambiguous rules and guidelines will support the growth of trust in a cultural diverse network, and prevent potential problems with conflict of interest.

6.2 Recommendations

There are several good practice guides to building information sharing network that should be consulted (see the end of the section), and any recommendations should be viewed in light of the goal and vision of the network in question. All our findings are not necessarily essential for the particular network in question.

Goal: Have a clear goal for the network, and make the role of every participant clear. The goal must be conveyed in a manner for everyone to understand. Answer questions like "who are welcome as members?", "what's in it for the members/which cost-benefit analysis can be present to the management?", "what kind of data will be shared?".

Goal: The network should be perceived as something trustworthy. Have clear and trusted communication channels and a PR strategy, not all PR is good PR, and you want to attract responsible members with the right attitude.

Goal: Know what to do when the network grows big. Should the network consist of delegates only? Shall the network be focused on the trust and the detailed work be performed in subgroups? If so-how will you support these working groups?

Goal: Create an environment that does not alienate anyone, and limit the perceived differences and work together towards a common vision and common goals.

Goal: Include international partners to help assist in the creation process. This can ensure that appropriate respect for cultural differences are adhered. Identify suitable governance model and a method of obtaining leader(s), and consider whether the leadership should be rotating.

Funding: Be clear on the planned funding and desired member types and prepare to make agreements to avoid possible conflicts of interest. This is particularly important if including law enforcement.

Funding/Members: If the network should include teams that might need financial assistance to participate, consider using network mechanisms for this. For example having a common funding arrangement or letting these member host events.

Members: Have clear network acceptance rules, included vetting. Urge the potential members to be frank about what they bring to the table. Tabs should be kept on members to make sure they have not interchanged personnel, whether all members still have other members willing to vet them and whether they still deliver the same services. The "vetting matrix" may very well be open and visible to at least the network members.

Members: Make the network restricted and exclusive to a reasonable limit. The key is to create a sense of togetherness and a common group feeling, not to intimidate non-members. If you are unnecessarily restrictive, you can be perceived as obstructing cooperation and making the network seem more "important" than it is.

Members/Activity: Build on existing contacts to have someone that can pull the weight from within. The best thing is if this group has resources and are willing to share information at

several levels, this could make them a “leading star”, having someone volunteering information can be a catalyst. People copy the behavior of their surroundings.

Activity: Set up a meeting schedule well in advance to keep costs down and promote predictability. If face-to-face meetings are too inconvenient, use other means to keep continuous contact. Remember to consider time zone differences when setting up on-line or telephone meetings.

Activity: Ensure everyone gets feedback. Feedback promotes initiative. Nothing is as uninspiring as total silence after posing a question. Convey these message to teams you trust can help create a good feedback loop as role models. Make sure that also content of little informational level receives proper feedback. The ones sharing need feedback to be encouraged to share more, and the ones who have not shared yet will be not be discouraged by “performance anxiety”.

Activity: Organize exercises. This can be to make sure the information sharing framework is understood and functioning, to make sure teams have exchanged current keys, to see that teams actually respond on the given contact addresses or just as a team building event to have members meet work closer together.

Activity: Organize social events in the network context, and do not make insensitive dietary decisions.

Activity/Rules: Have clear guidelines for activity level and meeting attendance. It can be anything from one email a month to 75% meeting attendance. One must consider the members’ economical situation and proximity to the meetings before demanding attendance.

Rules: Maintain a “code of conduct” list, the maintainers should represent a relevant cultural diversity. This list can consist of elements like “sharing business cards are appreciated” to “speaking out of turn is considered very rude” or “please do not use first names only”

Rules: Thoroughly educating network members in the governing guidelines, rules and regulations is imperative to avoid breaches caused by mistakes.

Rules: Promote transparency, discourage gossip, encourage gentle frankness. It is better to ask a person “how would you do it” than guessing.

Rules: Use a framework for information sharing, demand users to use PGP, or equivalent, in communication to ensure authenticity. Make sure the framework is not too complicated or rigid. Even if it is just email lists + PGP, it is still contained if the lists are vetted. If the framework is too complicated, people avoid using it, either by not sharing or by sharing insecurely.

Rules: Use a classification scheme like TLP to identify data sensitivity level to make sure everyone knows what to do and what not to do with received information, and also to bring attention to information classification.

Rules: Make clear statements about the policy for breaches of confidence. In the case of a breach, establish the gravity of the incident with the data owner. Enable a explanatory meet-

ing between the parties and function as mediator if need be. When it is resolved, inform the network to avoid rumors. Make sure you find the reason for the breach, it might be a symptom of something else.

Be positive, engaged and patient. Building trust takes time.

AP-CERT has done some good policy-work (http://www.apcert.org/). Nöster et al.[88] has important elements, and the GAO report[89] is definitely worth studying. Both the GAO and the ISAC recommendations[90] go deeper into specifications than is our intention here. Finally, we would like to mention ENISA's Best Practices[82] as an important document in the area.

6.3 Limitations

The research done for this thesis has some possible limitations apart from the ones discussed under mentioned under "Choice of method", p. 6.

The interviewer is not an experienced as such, hence the questions might have been leading or maybe not thorough enough. The interview itself might not have been conducted optimally, also on account of the lack of experience. The questions were tested on subjects before they were used in the interview, but they could have been tried on experts in the field to see if elements were likely to bring the interview into the wrong track. However, we feel that the interviewer's position as a professional peer created a good atmosphere, and grounds for a good fellow understanding during the interviews.

In an interview situation, political correctness may come in the way, as most people want to be perceived as open minded and accepting. Elements that could in some way put the interviewee in a bad light, might thus have been left out.

The literature was not extensive on the area in question in the thesis so quite a few articles are about areas we consider analogous enough for reference, for example cooperation between commercial companies. There might be a question about applicability of certain theories, as for instance issues in commercial companies might not always be transferable to trust networks, because there are other factors that influence the results.

Our results are not applicable to all trust networks, and the diversity in trust network composition is not treated as this is far too big a topic. Also the definition of trust could have been discussed more thoroughly as there is a vast amount of trust definitions depending on which field we are looking at: sociology, psychology, economics etc, Rousseau et al[18]. What we call "real trust" as a goal for information sharing is probably closest to "functional trust" in this literature, but we prefer the term experience-based trust.

6.4 Future work

Since this thesis was a broad study, several of the areas would be suitable for further work. First of all, a study including a more varied set of participants could prove interesting, having many different cultures represented. Elements like "cultural differences in recovering from breaches of trust" is another exiting theme, or looking closer at cultural differences that are relevant in

trust networks. Also useful could be looking more closely at the variations in what type of cyber incident information someone would be willing to share depending on group size and cultural background.

Exploring the effects of different kinds of trust, and to consider the effects of “reputation” and “popularity” on information sharing is an area for further exploration. Also looking into the area of organizational trust and conscious vs. unconscious aspects of trust could be of interest.

The sections on trust dynamics were fairly theoretical, and some experimental studies in this area would be interesting, as well as looking more closely at existing hierarchical networks and the functionality to further confirm or refute our claims.

The forming of a virtual crisis team from an existing trust network is something we omitted, but there are certainly an area of interest, and this could include suggested exercises and other, more general recommendations.

The set of recommendations here, together with other documentation in the field, could also be compiled into a full set of recommendations for trust networks.

A topic barely touched upon here is the economical consequences of demanding face-to-face meetings. We mentioned some possible solutions, but another discussion emerges from this: Who owns the responsibility of the security in a nation, considering that companies, network- and service providers are multi-national? Who should fund the security work: companies, government, service providers or “the security community”?

Looking into criminal trust networks to make comparisons would be both interesting, and potentially rewarding. This is, however, neither easily accessible nor risk-free.

Lastly, the effect of certification on trust can be evaluated, and the exploring of a possibly more transparent or visible vetting structure for reassurance in a network.

Bibliography

[1] CYBEX. 2010. Draft recommendation itu-t x.1500: Cybersecurity information exchange framework. *Editors of the CYBEX Correspondence Group, study group 17*, Telecommunication Standardization Sector.

[2] Jøsang, A., Hayward, R., & Pope, S. 2006. Trust network analysis with subjective logic. *Proceedings of the 29th Australasian Computer Science Conference*, 48.

[3] Servida, A. 2009. Towards a EU policy on critical information protection (CIIP). *Presentation, European Commision, DG INFSO-A3*.

[4] De Dreu, C. K. W., Giebels, E., & Van de Vliet, E. June 1998. Social motives and trust in integrative negotiation: The disruptive effects of punitive capability. *Journal of Applied Psychology*, 83(3).

[5] Hämmerli, B. M. 2009. Trust as a basis for collaboration. *Presentation, CEPS EU - CIIP*.

[6] Askheim & Grenness. 2008. Kvalitative metoder for markedsføring og organisasjonsfag. *Universitetsforlaget*.

[7] Kvale, S. 2001. Det kvalitative forskningintervju. *Ad notam, Gyldendal forlag*.

[8] Eisner, E. W. 1993. Forms of understanding and the future of educational research. *Educational researcher*, 22(7).

[9] Shaw, M. E. 1961. Group dynamics. *Annual Review of Psychology*, 12(1).

[10] Zucker, L. G. 1986. Production of trust: Institutional sources of economic structure. *Research in Organizational Behavior*, 8.

[11] Doney, P. M., Cannon, J. P., & Mullen, M. R. July 1998. Understanding the influence of national culture on the development of trust. *The Academy of Management Review*, 23(3).

[12] Ruohomaa, S. & Kutvonen, L. 2005. Trust management survey. *TRUST MANAGEMENT - Lecture Notes in Computer Science*, 3477.

[13] Abdul-Rahman, A. & Hailes, S. 1997. A distributed trust model. *NSPW Proceedings of the workshop on New security paradigms*.

[14] Msanjila, S. S. & Afsarmanesh, H. 2008. Inter-organizational trust in VBES. *Methods and tools for collaborative networked organizations*.

[15] Mayer, R. C., Davis, J. H., & Schoorman, F. D. July 1995. An integrative model of organizational trust. *The Academy of Management Review*, 20(3).

[16] Grandison, T. & Sloman, M. October 2000. A survey of trust in internet applications. *Communications Surveys & Tutorials, IEEE*, 3(4).

[17] Rosseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. 1998. Not so different after all: A cross-discipline view of trust. *The Academy of Management review*, 23(3).

[18] Msanjila, S. S. & Afsarmanesh, H. 2007. Towards establishing trust relationships among organizations in VBEs. *IFIP Advances in Information and Communication Technology*, 243.

[19] Cosimano, T. F. 2004. Financial institutions and trustworthy behavior in business transactions. *Journal of Business Ethics*, 52(2).

[20] Jøsang, A., Gray, E., & Kinateder, M. 2006. Simplification and analysis of transitive trust networks. *Web intelligence and agent systems*, 4(2).

[21] Massa, P. & Avesani, P. 2005. Controversial users demand local trust metrics: An experimental study on epinions.com community. *Proceedings of the National Conference on Artificial Intelligence*.

[22] Dasgupta, P. 2000. Trust as a commodity. *Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, Chapter 4, pp. 49-72*, Retrieved 2011-01-10, http://www.sociology.ox.ac.uk/papers/dasgupta49-72.pdf.

[23] Deutsch, M. December 1958. Trust and suspicion. *The Journal of Conflict Resolution*, 2(4).

[24] Jarvenpaa, S. L., Knoll, K., & Leidner, D. E. March 1998. Is anybody out there?: Antecedents of trust in global virtual teams. *Journal of Management Information Systems - Special section: Managing virtual workplaces and teleworking with information technology*, 14(4).

[25] Bachmann, R. March 2001. Trust, power and control in trans-organizational relations. *Organization Studies*, 22(2).

[26] Kramer, R. M. 1999. Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology*.

[27] Yuki, M., Maddux, W. W., Brewer, M. B., & Takemura, K. January 2005. Cross-cultural differences in relationship-and group-based trust. *Personality and Social Psychology Bulletin*, 30(1).

[28] Loss, L., Schons, C., Neves, R., Chudzikiewicz, I., & Vogt, A. 2007. Trust building in collaborative networked organizations supported by communities of practice. *IFIP Advances in Information and Communication Technology*, 243.

[29] Niu, J. 2006. Circles of trust: a comparison of the size and composition of trust circles in Canada and in China. *Thesis (Ph.D.) - Carleton University*.

[30] Elahee, M. N., Kirby, S. L., & Nasif, E. November 2002. National culture, trust, and perceptions about ethical behavior in intra- and cross-cultural negotiations: An analysis of CNAFTA countries. DOI: 10.1002/tie.10049.

[31] Larzelere, R. E. & Huston, T. L. August 1980. The dyadic trust scale: Toward understanding interpersonal trust in close relationships. *Journal of Marriage and Family*, 42(3).

[32] Pardo, T. A., Gil-Garcia, J. R., & Burke, G. B. 2006. Building response capacity through cross-boundary information sharing: The critical role of trust. *Exploiting the Knowledge Economy: Issues, Applications, Case Studies*.

[33] Zand, D. E. June 1972. Trust and managerial problem solving. *Administrative Science Quarterly*, 17(2).

[34] Smith, J. & Barclay, D. W. January 1997. The effects of organizational differences and trust on the effectiveness of selling partner relationships. *The Journal of Marketing*, 61(1).

[35] Kerr, M., Stattin, H., & Trost, K. 1999. To know you is to trust you: Parents' trust is rooted in child disclosure of information. *Journal of Adolescence*, 22(6).

[36] Butler Jr., J. K. June 1999. Trust expectations, information sharing, climate of trust, and negotiation effectiveness and efficiency. *Group Organization Management*, 4(2).

[37] Messenger, M. 2005. Why would i tell you? Perceived influences for disclosure decisions by senior professionals in inter organisation sharing forums. MSc Organisational Behaviour.

[38] Mullins, B., Lacey, T., Mills, R., Trechter, J., & Bass, S. 2007. How the cyber defense exercise shaped an information-assurance curriculum. *Information Security*.

[39] Khambatti, M., Dasgupta, P., & Ryu, K. D. April 2004. A role-based trust model for peer-to-peer communities and dynamic coalitions. *IEEE International Information Assurance Workshop*, 2.

[40] Levin, D. Z. & Cross, R. November 2004. The strength of weak ties you can trust: The mediating role of trust in effective knowledge transfer. *Management Science*, 50(11).

[41] Ruuska, I. & Vartiainen, M. 2003. Communities and other social structures for knowledge sharing: a case study in an internet consultancy company. *Communities and technologies*, ISBN:1-4020-1611-5.

[42] Hämmerli, B. & Renda, A. February 2010. Task force critical (information) infrastructure protection in Europe. *Minutes from CEPS, Brussels meeting*.

[43] Kimble, C., Barlow, A., & Li, F. September 2000. Effective virtual teams through communities of practice. *University of Strathclyde Management Science Research Paper*.

[44] Bowles, S. & Gintis, G. February 2000. Optimal parochialism: The dynamics of trust and exclusion in networks. *Department of Economics Working Paper Series, Paper 68, University of Massachusetts*.

[45] Brewer, M. B. 1996. Ingroup favoritism: the subtle side of intergroup discrimination. *Codes of conduct: behavioral research into business ethics*.

[46] Barber, B. 1983. The logic and limits of trust. *Rutgers University Press*.

[47] Fine, G. A. & Holyfield, L. March 1996. Secrecy, trust, and dangerous leisure: Generating group cohesion in voluntary organizations. *Social Psychology Quarterly*, 59(1).

[48] Guardiola, X., Guimera, R., Arenas, A., Diaz-Guilera, A., Streib, D., & Amaral, L. A. N. June 2002. Macro- and micro-structure of trust networks. *arXiv*, cond-mat/0206240v1.

[49] Thomas, E. J. February 1959. Role conceptions and organizational size. *American Sociological Review*, 24(1).

[50] Brewer, M. B. & Kramer, R. 1986. Choice behavior in social dilemmas: Effects of social identity, group size, and decision framing. *Journal of Personality and Social Psychology*, 50(3).

[51] Audestad, J. A. 2008. E-bombs and e-grenades, the vulnerability of the computerized society. *MiS Course Literature IMT 4481, Gjøvik University College*.

[52] Lave, J. & Wenger, E. 1991. Situated learning: legitimate peripheral participation. *Cambridge University Press*.

[53] Wenger, E. & Snyder, W. Jan-Feb 2000. Communities of practice: The organizational frontier. *Harvard Business Review*.

[54] Brown, J. S. & Gray, E. S. October 1995. The people are the company. *Fast Company*, 1(1).

[55] McDermott, R. & O'Dell, C. 2001. Overcoming cultural barriers to sharing knowledge. *Journal of Knowledge Management*, 5(1).

[56] Loss, L., Schons, C. H., Neves, R. M., Delavy, I. L., Chudzikiewicz, I. S., & Vogt, A. M. C. 2007. Trust building in collaborative networked organizations supported by communities of practice. *IFIP Advances in Information and Communication Technology*, 243.

[57] Wolf, P. & Kazi, A. S. 2006. Communities of practice: A case study from the automotive industry. *RealLife Knowledge Management: Lessons from the Field*, KnowledgeBoard, ISBN: 9525004724.

[58] Gelfand, M. J., Erez, M., & Aycan, Z. January 2007. Cross-cultural organizational behavior. *Annual Review of Psychology*, 58.

[59] Wall, J. A. June 1975. Effects of constituent trust and representative bargaining orientation on intergroup bargaining. *Journal of Personality and Social Psychology*, 31(6).

[60] Kasper-Fuehrera, E. C. & Ashkanasy, N. M. June 2001. Communicating trustworthiness and building trust in interorganizational virtual organizations. *Journal of Management*, 27(3).

[61] Klijn, E.-H. 2009. The challenges of network management: coordinating, mediating and building trust in networks. *Zurich Roundtable on Comprehensive Risk Analysis and Management*, Retrieved 2011-03-02, http://e-collection.library.ethz.ch/eserv/eth:2303/eth-2303-01.pdf.

[62] Kenis, P. 2009. Introduction to the network governance approach. *Zurich Roundtable on Comprehensive Risk Analysis and Management*, Retrieved 2011-03-02, http://e-collection.library.ethz.ch/eserv/eth:2303/eth-2303-01.pdf.

[63] Williams, S. 2004. Building and repairing trust. *LeaderLetter, Wright State University*, Retrieved 2010-11-23, http://www.wright.edu/ scott.williams/LeaderLetter/trust.htm.

[64] Kim, P. H., Ferrin, D. L., Cooper, C. D., & Dirks, K. T. February 2004. Removing the shadow of suspicion: the effects of apology versus denial for repairing competence-versus integrity-based trust violations. *Journal of Applied Psychology*, 89(1).

[65] Moberg, L., Kringen, J., Nordvik, J.-F., & Strøm, M. Himmelen, havet og sannheten, kritisk analyse av tilsynsordninger. *DIFI: Direktoratet for Forvaltning og IKT*, Retrieved 2011-09-05, http://www.difi.no/statskonsult/publik/bokhefteveil/tilsyn/tilsyn.pdf.

[66] ENISA. 2010. Incentives and challenges for information sharing in the context of network and information security. *Resilient e-Communications Networks*, Retrieved 2011-02-15 from http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/.

[67] Gal-Or, E. & Ghose, A. June 2005. The economic incentives for sharing security information. *Information Systems Research*, 16(2).

[68] Kolekofski Jr., K. E. & Heminger, A. R. July 2003. Beliefs and attitudes affecting intentions to share information in an organizational setting. *Information & Management*, 40(6).

[69] Constant, D., Kiesler, S., & Sproull, L. December 1994. What's mine is ours, or is it? A study of attitudes about information sharing. *Information Systems Research*, 5(4).

[70] Falcone, R. & Castelfranchi, C. 2001. The socio-cognitive dynamics of trust: Does trust create trust? *Lecture Notes in Computer Science*, 2246.

[71] W.J. Schepens, W. J., Schafer, J., Ragsdale, D. J., & Surdu, J. R. 2003. The cyber defense exercise: An evaluation of the effectiveness of information assurance education,. *BlackHat proceedings*, Retrieved 2011-01-10, http://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-dodge.pdf.

[72] Trimintzios, P. 2011. Cyber Europe 2010, evaluation report. *ENISA publication*, Retrieved 2011-08-08, http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report.

[73] Conklin, A. & White, G. B. january 2006. E-government and cyber security: the role of cyber security exercises. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 39.

[74] Lane, C. June 1996. Industry and society in Europe: stability and change in britain, germany and france. *Industrial Relations Journal*, 27(2).

[75] Alesina, A. & La Ferrara, E. 2002 November. Who trusts others? *Journal of Public Economics*, 85(2).

[76] Luo, Y. August 2005. How important are shared perceptions of procedural justice in cooperative alliances? *The Academy of Management Journal*, 48(4).

[77] Zaheer, A., McEvily, B., & Perrone, V. March-April 1998. Does trust matter? exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science*, 9(2).

[78] Tsai, W. August 1998. Social capital and value creation: The role of intrafirm networks. *The Academy of Management Journal*, 41(4).

[79] Data sharing protocol. *UK Ministry of Justice*, Retrieved 2011-01-15 http://www.justice.gov.uk/guidance/freedom-and-rights/data-sharing.htm.

[80] 2006. Department of health: Making a difference: Safe and secure data sharing between health and adult social care staff. *UK Department of health*, Retrieved 2011-01-15 from http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/.

[81] ENISA. A Framework for Information SHaring and Alerting (FISHA). *CERT Polska, CERT-Hungary and the University of Gelsenkirchen, EPCIP programme*, Retrieved 2011-03-17 http://fisha-project.eu/the-project.

[82] Ouzounis, V. Good practice guide. *ENISA*, Retrieved 2011-09-01 from http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/.

[83] Camarinha-Matos, L. M. & Afsarmanesh, H. 2007. A comprehensive modeling framework for collaborative networked organizations. *Journal of Intelligent Manufacturing*, 18(5).

[84] Brunner, E. & Suter, M. 2010. Evaluation und weiterentwicklung der melde- und analysestelle informationssicherung schweiz melani 2010. *ETH Zurich*, Retrieved 2011-03-10 from http://www.isn.ethz.ch/isn/Digital-Library/Publications/.

[85] Connaster, B. R. 1999. Last rites for readability formulas in technical communication. *Journal of Technical Writing and Communication*, 29(3).

[86] Schmidt, V. October 2010. The unfinished architecture of Europe's economic union. *Governance*, 23(4).

[87] Rosecrance, R. 2010. Capitalist influences and peace. *International Interactions*, 36(2).

[88] Nöster, M., Gruber, M., & Feindt, S. January 2006. How to initiate cooperative networks - practical guidelines for industry associations, development agencies and SMEs. *Online publication*, Retrieved 2010-12-05, http://www.tages.biz/news/implementationguide.pdf.

[89] GAO. October 2001. Information sharing: Practices that can benefit critical infrastructure protection. *United States General Accounting Office*, Retrieved 2011-02-07 http://www.gao.gov/products/GAO-02-24.

[90] ISAC. January 2004. Vetting and trust for communication among ISACs and government entities. *ISAC Council*, Retrieved 2010-09-16, http://www.isaccouncil.org/.

A Acronyms and abbreviations

AAAI	American Association for Artificial Intelligence
APCERT	Asia Pacific Computer Emergency Response Team
CEPS	Centre for European Policy Studies
CERT	Computer emergency Response Team
CI	Critical infrastructure
CIIP	Critical Information Infrastructure Protection
CoP	Communities of Practice
CSIRT	Computer Security Incident Response Team
DIFI	Direktoratet for forvaltning og IKT
EGC	European Government CERTs
ENISA	The European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
FIRST	Forum of Incident response and Security teams
FISHA	Framework for Information Sharing and Alerting
IEEE	Institute of Electrical and Electronics Engineers
ISAC	Information Sharing and Analysis Centers
ITU-T	International Telecommunications Union, Telecommunication Standardization Sector
Melani	Melde- und Analysestelle Informationssicherung
NAFTA	The North American Free Trade Agreement
NBER	National Bureau of Economic Research
NDA	Non-Disclosure Agreement
OIC-CERT	The Organisation of the Islamic Cooperation – Computer Emergency Response Team
OPSEC	OPerational SECurity
Parsival	Protection and Trust in financial structures
POC	Point Of Contact
SIG	Special Interest Group
Terena	Trans-European Research and Education Networking Association
TI	Trusted Introducer
TLP	Traffic Light Protocol
TTP	Trusted Third Party

B The original questionnaire

Several follow-up questions are not included in the questionnaire, some done on site, some sent later

Questionnaire outline:
If the network grows too big for personal relationships: how do you maintain trust?
How can we remedy a diminishing trust due to group size and is restructuring of the group is a solution, with all the possible complications this might introduce?

If an event diminishes trust, e.g. personal breach of confidence, personal job switches, political changes etc., how do you deal with the change in trust level?
Do certain repercussions restore the trust level or is a restructuring of the group in order, that is; is the trust level automatically lowered? Do these conclusions differ greatly from group to group depending on the mandate and member types?

Do Cultural differences inhibit trust in a trust network?
Do cultural elements, culture being anything from religion to the local national culture in dealing with for instance rogue ISPs inhibit trust in certain security peers, hence inhibit information sharing and how can this possible be remedied?

Questionnaire:
Section1
If the network grows too big for personal relationships: how do you maintain trust?
Hypothesis: There is a size limit to trust and real trust is not possible in large groups.

1. Do you feel that there is some fixed maximum size of trust networks (examples are FIRST with 236 members, Trusted Introducer with 75 members or MELANI with 200 members)?
   1. (Yes) Why is there a size limit?
      1. Is it because of lack of personal relationships?
      2. Is it because of lack of proper governance or leadership?
      3. Would clear rules and outspoken policies remedy some of the trust problems (or is this just a structure)
   2. (No) Do you believe you would share sensitive info with someone you have not met?
      1. What if you do not even know the person who recommended them?
      2. So you trust network itself, then?

2. How do you feel we can remedy a diminishing trust due to group size?

3. Restructuring of the group is a solution, but that leaves several options open, like
   1. Splitting into smaller groups. If you think this is a solution, how do you think this should be done
      1. Cultural
      2. Sector-wise
      3. Geographical
      4. Common problem area groups exist (e.g. phishing, spam, IDS, information sharing), does this not suffice or do they also grow to big?
      5. Would the lack of variation in the composition of the group be an asset or a disadvantage?
   2. One could see a delegate or representation model, like country CERT forum? If so how
      1. Sector?
      2. Geographic?
   3. Would the delegate model influence the competence level of the group? (e.g. if one country has extraordinary many anti phishing initiatives but only one representative and another country has no competence but still a representative)

4. Do you think a delegate model would lead to less variation in a group?
5. How would you make sure a constituency has sufficient trust in a delegate, or that the delegate trusts what it receives from the constituency?
    1. Is this also boiling down to personal relationships?
    2. How important would you consider respect from the constituency in the competence of the delegate is here?
6. How do you make someone give up their personal representation and the power that this gives?
7. Do you believe that it is important to people to be recognized for their competence?
    1. How would they be recognized as competent if they are represented by someone else?
8. What consensus level is needed behind a delegate? Should this be a rule or optional?

Section 2

If an event diminishes trust, e.g. personal breach of confidence, political changes etc., how do you deal with the change in trust level?
Hypothesis: The trust level in trust networks is dynamic and the network should adapt to this.

We will take an example event: breach of trust of one of the participants, maybe too broad sharing of incident information.

1. Do you feel that the network should punish in some way?
    1. (If yes:) Who will be punished, the team or the rep? How do you distinguish?
    2. (If yes:) What kind of punishment? Exclusion? Probation?
    3. (If yes:) Would this give the leadership/governance judicial character that could conflict with a nation's law regulations?
    4. Would you trust anyone more after they have been punished?
    5. Are trust and punishment at all related? (example; children)
2. Would the representative or person in question have to be replaced?
3. Will the level of trust start lower after en incident?
4. Do you think steps should be taken to ensure the network of a trust level following an incident like this or is natural growth over time sufficient?
5. People switch jobs, and if the person in a network represents the workplace, the representative has to be switched.
    1. How do you feel this affects the trust level?
    2. Do you think steps should be taken to ensure the network of a trust level following an incident like this or is natural growth over time sufficient?
6. Do you think political instability could influence the trust level?
    1. Do you think steps should be taken to ensure the network of a trust level following an incident like this or is natural growth over time sufficient?
7. Would clear rules and outspoken policies help increase trust or are these dynamics in trust level natural and should just be expected and accepted?
8. How do you think the network would react if reps form smaller groups with higher trust level as a spawn of the original network?
    1. Would people feel left out?
    2. Would it affect the trust level in the original network?
9. What consensus level in a trust network is needed to accept either a change of trust level or a punitive action?
10. Would the restoration of trust in a specialized group differ from that of a cross discipline network? E.g. in a banking or energy grid network vs. FIRST or TI.
11. If the change in trust level occurs in a group that uses a deputy model, would this come out differently?

12. The network trusts the deputy, but would it affect the trust if there was a breach with one of the parties in the constituency of this representative?
13. How should the leadership/governance of groups work in order to aid the trust level adjustment? (or is personal trust and trust in competence still the real governance factors)

Section 3
Question: Do Cultural differences inhibit trust in a trust network?
Hypothesis: Even in trust situations there are some cultural differences that take priority and inhibits the flow of information.

An example situation: One country that has displayed rogue network elements, many untrustworthy ISPs hosting botnet C&Cs etc.

1. Does this affect your trust in a representative from this country?
    1. Does the rep have to prove himself?
    2. Would it take longer time for a trust level to be restored?
2. Would strong rules and outspoken policies compensate for some of these issues? (or is the personal relation and competence respect the main factors here too)
3. How long would you guess it takes to make a personal relation good enough, through meetings, given you live far apart?
4. How important is the trust in competence here?
    1. How would you test the competence?
    2. How about in a deputy model, would you expect the same competence?
5. How about openness factors, some cultures are more used to sharing information than others, how do you factor this in?
6. Would clear rules and outspoken policies be sufficient to battle such differences?
    1. Do you think the constituency would accept a sharing of their information from these rules?
7. Do you think strong religious differences could be an inhibitor?
    1. Do you think religious based coalitions are helpful or harmful? For instance Islamic CERT.
        1. Why?
8. How important would leadership/governance in the group be to avoid these cultural speed bumps to information exchange?